Regulamentação da Web

PATRICIA PECK PINHEIRO

REGULAMENTAÇÃO DA WEB

■ A Sociedade humana desenvolveu há muito tempo um modelo harmônico de convivência social baseado em um sistema de regras de conduta. Segundo Jean Dabin, advogado e filósofo belga, só há que se falar de uma relação legal se há uma relação social, quando existe uma sociedade organizada.

Inicialmente, estas regras eram transmitidas de forma oral, mas rapidamente o sistema evoluiu para um formato escrito e documentado. Isso porque um dos fatores principais para o sucesso de qualquer regulamentação é que a norma comportamental precisa estar clara, ser objetiva, para conseguir ser imposta a uma coletividade.

Ademais, com o passar do tempo também foi aprimorado o método de criação deste conjunto de regramentos para que fosse também socialmente aceito, legítimo, até chegarmos no cenário atual do Poder Legislativo.

A motivação para todo este desenho jurídico-social é o estabelecer um melhor relacionamento social entre os homens. A partir do momento que o indivíduo sabe previamente qual a postura recomendada, qual comportamento é esperado e desejado pela comunidade na qual está inserido, tem então o livre-arbítrio de escolher entre cumprir com a regra ou não, e no último caso sofrer com as consequências previstas, chamadas de sanção.

Sendo assim, independente do avanço tecnológico, a necessidade de se estabelecer parâmetros e limites para as atitudes humanas é uma condição para a própria vida em sociedade. A garantia das liberdades depende do cumprimento deste compromisso, deste pacto social.

Dito isso, desde a criação da Internet, uma das maiores discussões é justamente sobre a necessidade ou não de se regulamentar este ambiente que teria, em princípio, surgido, sem qualquer controle impositivo. Por certo, quanto maior o número de usuários de uma determinada ferramenta, maior a necessidade de se estabelecer um código de conduta.

Foi o que ocorreu com o automóvel, que hoje, após seu uso massificado, passou a exigir não apenas uma habilitação, ou seja, um treinamento prévio para capacitar o usuário, como também o atendimento a um conjunto de normas obrigatórias, que sujeitam a penalidades que vão de multa até a perda do direito de dirigir.

Então, seguindo esta linha de raciocínio, após aproximadamente 50 anos da invenção da Arpanet, que foi o embrião do mundo digital que vivemos hoje, vemos a necessidade de construir regras mais claras para seu uso ético, seguro, legal, saudável e sustentável. Mas com um novo desafio, que é a quebra do paradigma geográfico na aplicação da norma legal.

Portanto, todos os operadores envolvidos na viabilização do universo digital, materializado nas interfaces do "www", e de seus desdobramentos mais recentes até a chegada dos aplicativos, devem coordenar esforços para padronizar o que deve ser seguido por todos neste ambiente, de usuários às instituições, onde quer que estejam.

Logo, o primeiro e talvez maior desafio a ser enfrentado tem relação direta com a própria natureza da web, que é a ausência de limitação territorial. Contrariando o modelo estabelecido até então em que as leis se aplicam dentro de determinados limites geográficos, em respeito à soberania dos Estados.

Mas não é a primeira vez que vivenciamos isso, vide a necessidade recorrente de se estabelecer Tratados e Convenções Internacionais entre os países e seus cidadãos.

O primeiro passo neste sentido foi dado quando da definição do padrão de protocolo TCP/IP e criação de Comitês Gestores de Internet em todo o mundo, com a missão de articular a melhoria evolutiva da mesma, bem como os requisitos necessários para a sua interconectividade e integração.

A partir daí, o crescimento foi tão acelerado que andou mais rápido o estabelecimento de regras através de contratos privados, ou seja, criadas pelos fornecedores de serviços da Internet e traduzidas em Termos de Uso, que representam um modelo de auto-regulamentação como ocorre com o regimento interno de um condomínio, uma escola, ou um clube.

Ou seja, o primeiro avanço para regulamentação da web foi realizado pela iniciativa privada e não pelo poder instituído. Estes códigos de conduta digitais estão espalhados por toda a Internet, para tudo que se queira fazer. No entanto, ainda utilizam um formato precário de linguagem essencialmente jurídica, deixando de tomar proveito do potencial multimídia da rede que permite uma abordagem mais didática e educativa.

Afinal, uma regra que ninguém lê, logo, desconhece, tem pouca eficácia preventiva e acaba só tendo utilidade quando há um desfecho judicial. Isso fez com que, nos últimos anos, com o aumento vertiginoso de usuários, a Internet tenha se tornado um local selvagem, como se tivéssemos voltado ao estado de natureza, onde vale a lei do mais forte, ou ainda a lei de Talião, olho por olho, dente por dente, com as pessoas fazendo justiça com o próprio mouse.

Devido justamente a este caos, os sistemas jurídicos de todo o mundo iniciaram uma cruzada para elaborar e/ou atualizar as leis de modo que estas alcançassem melhor as situações e condutas surgidas com o advento deste ambiente de relacionamentos digitais atemporais e multiterritoriais.

Sendo assim, a maioria dos países passou a discutir e aprovar regras novas, mais condizentes com esta atual realidade. Em alguns casos, inclusive, foram criadas Diretivas para tratar uniformemente alguns temas mais essenciais tais como neutralidade, liberdade de expressão, privacidade, proteção de dados pessoais, crimes eletrônicos, consumidor online, comércio eletrônico, proteção de direitos autorais digitais, entre outros.

Cada país no seu ritmo, e o Brasil de forma mais lenta, promulgou leis com o objetivo de regulamentar melhor a web. Algumas bem intencionadas, outras desastrosas. Isso porque a premissa basilar da Internet tem a ver com o fato de que não é uma outra realidade, paralela, chamada de virtual, ou cibernética.

Vivemos um uma Sociedade única, e as condutas devem ser tratadas com certa equidade, quer tenham ocorrido de forma presencial ou à distância, pela via analógica ou pela via digital. E nesta última hipótese, não importa que tecnologia seja inventada para viabilizar relações e obrigações entre partes ausentes, do telex, ao telefone, ao celular, à internet.

Tratar a Internet como um mundo à parte é um dos maiores erros que pode ser cometido pelos estrategistas jurídicos. Por certo, a tecnologia trouxe algumas situações novas, ainda não previstas pelas leis existentes, pois afeta e altera o comportamento dos indivíduos.

Antes de inventarem o carro não havia o acidente de carro. Antes da internet não havia um dano causado por “bug” ou por “vírus” de computador. Muito

menos um golpe de engenharia social baseado no envio de um email falso com a pegadinha "clique aqui no link".

Apesar de toda a inovação, o que mudou mesmo foi o *modus operandi*, a forma de executar determinada ação, seja ela lícita ou ilícita, mas não os valores que devem ser protegidos por um sistema jurídico-social. Por isso, princípios gerais do direito como "a ninguém lesar", "dar a cada um o que é seu" e "viver honestamente" são ainda tão válidos e aplicáveis, não importa quanto tecnológica a Sociedade tenha se tornado.

Provavelmente, o maior efeito que sentimos hoje está mais relacionado com a capacidade de informação, ou seja, saber o que está ocorrendo pois há maior documentação e prova das condutas.

Os crimes mais recorrentes do mundo digital são velhos conhecidos dos ordenamentos jurídicos, como os crimes contra a honra (injúria, difamação, calúnia), ameaça, discriminação, falsa identidade, falsidade ideológica, fraude.

A diferença é que agora tem mais evidências da ocorrência dos mesmos. E isso, por si só, já contribui para gerar um grande sentimento generalizado de insegurança dentro da Internet.

Isto porque a partir do momento em que há prova de um ato ou fato, nasce o dever de agir. E se não há uma resposta da autoridade competente para combater a prática ilícita, cresce a impunidade, que por sua vez estimula mais ilícitos.

O maior estímulo ao descumprimento de regras, por melhor que ela tenha sido feita, é a certeza da impunidade. No caso da Internet, o que mais tem contribuído para este quesito é a possibilidade do anonimato.

Desse modo, um dos pontos cruciais no meio digital é justamente evitar que alguém possa cometer atos sem ser identificado, ou pior, realiza-los fingindo ser outra pessoa. A confiança na identidade declarada é requisito para o crescimento da própria Economia Digital.

Ademais, há dois fatores agravantes nas condutas exercidas através da internet: primeiro a sensação de distanciamento que ela causa, que faz com que os atos sejam mais covardes e cruéis; segundo a sua amplitude, que tem dimensão global e pode se perpetuar no tempo.

Enquanto uma ofensa presencial gera um efeito e tem uma duração limitada no tempo, a mesma ofensa através da internet tem um poder danoso muito maior, ilimitado e inesgotável.

Logo, simultaneamente a vontade de construir um arcabouço legal de regras e limites para a vida digital, o acesso facilitado às novas tecnologias, por pessoas

cada vez mais jovem, fez crescer o perigo desta nova "praça pública" que estimula maior convivência de pessoas, de forma interconectada em tempo real.

Para desespero do poder público, o crime organizado tomou proveito desta oportunidade da Internet ter surgido inicialmente como uma "terra sem lei" para ampliar sua atuação, o que fez surgir a "Deep Web", que seria a internet obscura, que atraiu nos últimos anos de quadrilhas de fraudadores de cartões de crédito a terroristas.

Podemos afirmar que vivemos atualmente um estado primitivo de direito na Internet. O que pode ser feito então para proteger o bem público digital? Como instrumentalizar as regras de conduta para que sejam mais eficazes na Internet e com isso garantir maior segurança para todos os seus cidadãos-internautas?

No Brasil, a importância da regulamentação da web vem aumentando, com a promulgação de leis mais específicas como a Lei de Crimes Eletrônicos (Lei 12.737/2012) e a Lei do Marco Civil da Internet (Lei 12.965/2014). Além do andamento de diversos projetos de lei, entre eles o de Proteção de Dados Pessoais.

Estas duas leis brasileiras recentes, uma com ênfase criminal e outra civil, são um bom exemplo da dificuldade de se legislar sobre matérias mais técnicas, como as que envolvem a Internet.

Ambas tiveram longos períodos de tramitação no Legislativo, envolveram consultas públicas, e ao final, recepcionaram uma redação muito tímida se comparada com a relevância das pautas abordadas, seus propósitos e objetivos.

A atualização da norma penal é essencial, visto que na interpretação da mesma pelo Judiciário não é possível ser aplicada analogia. Ou o crime está bem tipificado, ou então a conduta não será enquadrada como crime.

Ademais, há diversos crimes que quando ocorrem através do meio digital merecem uma penalidade maior, visto que passam a ser mais graves e têm consequências maiores.

Sendo assim, para haver uma boa regulamentação da parte criminal, há necessidade de se alcançar estes dois objetivos: dar o devido tratamento às condutas novas, bem como revisar a penalidade das condutas que possuem um novo *modus operandi* digital.

A Lei "Carolina Dieckmann", como ficou conhecida, após mais de 10 anos de discussão, acabou por trazer apenas 4 artigos novos para o contexto legal nacional. Dentre estes, o mais relevante foi a adequação do artigo 154 do Código Penal para tratar do crime de invasão digital (redação nova do artigo 154-A e 154-B).

Pela nova lei, passou a ser crime invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de meca-

nismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Destaque-se que o crime tem um requisito, que é a violação indevida de um mecanismo de segurança. Ou seja, se o dispositivo não estiver bloqueado, por exemplo, com uma senha, não será possível determinar que houve violação.

Este ponto foi muito discutido para que se evitasse criminalizar a conduta proveniente de um acesso não intencional. No entanto, gerou um ônus para a vítima, que é o de ter que manter a "porta fechada" do seu equipamento.

Apesar da gravidade de um crime de invasão, a pena ficou muito branda, sendo de detenção de três meses a um ano, e multa. Podendo ser aumentada de um sexto a um terço se da invasão resultar prejuízo econômico.

A penalidade maior ficou para o caso em que haja extração de dados em consequência da invasão, que foi uma forma de tratar do furto de informações sem ser no artigo tradicional de furto que é o 155 do Código Penal.

Logo, se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido, a pena ficou de reclusão, de seis meses a dois anos, e multa, se a conduta não constituir crime mais grave. Podendo ser ainda aumentada de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.

Além deste crime, a lei fez mais duas atualizações singelas no Código Penal, acrescentando ao artigo 266 a hipótese de interrupção de serviço telemático ou de informação de utilidade pública, que vem em resposta às ações de retirada de sites públicos do ar, como ocorreu com a atuação do grupo "Anonymous". E atualizando o artigo 298 para abranger no rol de falsificação de documento particular a falsificação de cartão de crédito ou débito.

Infelizmente, ficaram de fora ajustes importantes para dar melhor tratamento às condutas de fazer arquivos maliciosos, artefatos e/ou vírus de computador, bem como o de estelionato digital que ocorre mediante o uso não autorizado de dados financeiros e/ou bancários de alguém na internet e que tem sido tratado como furto mediante fraude pela falta de um melhor enquadramento.

Traçando um comparativo com outros países, o Estado da Califórnia, nos EUA, vem dando tratamento rigoroso às condutas digitais mais danosas, como é o crime de falsa identidade praticado na criação de um perfil falso ("fake") na

Internet, com aplicação de multa de U$ 1.000 dólares e prisão de até 1 ano (seção 528.5 do Código Penal da Califórnia).

No Brasil, a situação da falsa identidade está tratada no artigo 307 do Código Penal, mas é um crime de penalidade leve, detenção de três meses a um ano ou multa. Poucos são os casos em que este tipo de conduta é de fato penalizada. E quando isso ocorre, a pena acaba convertida apenas no pagamento de uma cesta básica.

A falsa identidade é considerada um tipo de crime acessório, ou seja, um crime utilizado normalmente como meio para execução de outro crime mais grave. No entanto, na Internet, o mero fato de alguém se fazer passar por outra pessoa, por si só, já pode ser extremamente prejudicial para a vítima, mesmo que seja uma "brincadeira de mau gosto".

Pessoas públicas, celebridades, autoridades, políticos, alto escalão executivo, todos têm sido vítima de perfis falsos, mesmo que a título de protesto, devemos ter muito cuidado com a forma de manifestar a opinião pois os fins não justificam os meios.

Se por um lado a web possibilita que alguém possa facilmente se passar por outra pessoa, ela também dificulta bastante a prova de autoria quando necessária para impor uma obrigação ou uma sanção.

Um dos temas que mais merecem debate para dar melhor tratamento por parte do Estado ao combate do crime digital é justamente o sobre a necessidade de aperfeiçoamento da capacidade de prova de autoria de um ato ocorrido em meio digital.

Muitos casos ficam sem solução justamente pela dificuldade de se atribuir de forma inequívoca um ato à uma identidade. Ou seja, uma questão jurídica essencial para regulamentação da web envolve justamente a definição de um padrão único de identidade digital, não apenas no âmbito nacional, mas sim internacional.

A identificação de pessoas através de fronteiras é um dos controles mais primordiais para se garantir segurança coletiva e capturar criminosos foragidos.

Além disso, deve-se padronizar o tempo de guarda das evidências eletrônicas visto que para um único evento pode ser necessária apresentação de provas coletadas e armazenadas por várias máquinas que podem estar inclusive em países diferentes.

E este foi um dos pontos abordados pela Lei do Marco Civil da Internet, na questão do tratamento de guarda de logs (registros) de conexão e navegação na web.

Por último, além de se atualizar a lei penal, deve-se também melhorar a Lei de Execuções Penais, para que fique mais adequada a questão do encarceramento do criminoso digital.

Em muitos países, este novo tipo de bandido recebe um tratamento diferenciado, visto que apenas a prisão física restritiva de Liberdade não é suficiente para segurá-lo.

Ademais, alguns novos institutos passaram a ser tratados no tocante a regulamentação da web, que tem relação direta com a proteção dos direitos essenciais do cidadão digital. Entre eles, o da neutralidade, recepcionado nos artigos 3º. e 9º. do Marco Civil da Internet.

A neutralidade na internet significa, em resumo, garantir que não haverá discriminação ou privilégio no tráfego de dados. Ou seja, não haverá uma manipulação unilateral para atender interesses de alguns em detrimento dos demais, fazendo com que os dados de um trafeguem mais rápido e com melhor performance do que os dados de outro similar.

Há que se destacar, por oportuno, que o Marco Civil da Internet, em seus artigos 4º. e 7º., inovou ao elevar o direito de se conectar a web à categoria de direito essencial para o exercício da cidadania. Isso significa que esta recente regulamentação brasileira destacou do que seriam valores e direitos fundamentais do indivíduo da Sociedade Digital.

Apesar de bem intencionada, esta nova lei esbarra em alguns entraves técnico-jurídicos ainda intransponíveis, como é a previsão do artigo 11, que determina a aplicação da lei brasileira em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, desde que pelo menos um dos terminais esteja localizado no Brasil.

Este artigo aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

Para exemplificar, isso significa que se alguma empresa, de qualquer lugar do mundo, disponibilizar um aplicativo gratuito na loja da Apple ou da Google, e o mesmo venha a ser baixado por um brasileiro, vai aplicar a lei Brasileira por um dos terminais estar no Brasil, ou mesmo por haver troca de dados a partir do Brasil.

O que traz o dever de atender as demais previsões do Marco Civil da Internet, no tocante ao idioma necessariamente ter que ser o português nos Termos de Uso

dos Serviços (contrato), bem como haver possibilidade de o usuário solicitar exclusão da base de dados se deixar de ser cliente do serviço.

Ademais, haverá o dever de guarda de evidências eletrônicas geradas na aplicação web pelo prazo de 6 meses e se a conexão for a partir de um número de IP registrado no território nacional deve ser guardada a evidência desta conexão por 1 ano.

Por certo, há princípios universais do direito que devem também estar garantidos na Internet, como o direito à privacidade e a própria liberdade de expressão. Mas o desafio maior é como fazer isso usando técnicas tradicionais de uma época anterior a toda a Revolução Digital?

O Marco Civil da Internet tratou destes princípios, já recepcionados e garantidos pela Constituição Federal de 1988, mas deu tratamento preferencial à liberdade de expressão em detrimento a proteção da honra e reputação do indivíduo, na medida em que passou a determinar que um conteúdo só possa ser removido da web com ordem judicial.

Ou seja, independente do avanço de autogestão dos serviços digitais, como as Mídias Sociais, em que há uma mediação de conflitos realizada pela própria ferramenta, a lei brasileira priorizou a permanência do conteúdo publicado e compartilhado, excetuando apenas o caso de exposição de nudez não autorizada, que enseja remoção imediata a pedido do envolvido, de forma extrajudicial.

Mas será que o Legislativo e o Judiciário estão preparados para acompanhar esta dinâmica social tão transformadora? O tempo normal de tramitação nestas duas esferas é muito superior ao que um usuário está disposto a aguardar para ter seu direito garantido (seja por lei ou por decisão judicial).

Portanto, em última instância, a tendência de regulamentação da web exige rever o próprio modelo de criação de leis e de execução das mesmas. Afinal, se as partes podem estar em qualquer lugar, a qualquer momento, como trazer a discussão da causa para uma corte que exija a apresentação presencial dos envolvidos?

Talvez tenhamos que desenvolver um modelo que permita que haja toda uma tramitação também digital. O processo eletrônico do judiciário já é um primeiro avanço neste sentido, mas como já foi dito, não será possível alcançar a eficácia necessária para impor regras de conduta na Internet se isso ficar adstrito e limitado a um país.

Lawrense Lessig, professor de Direito de Harvard, já dizia que a transparência é a principal moeda da sociedade atual e que a tecnologia deve ser utilizada para passar a regra do jogo no próprio jogo. Por isso foi um dos precursores ao criar o modelo de licenças de direitos autorais chamado "Creative Commons" no

qual os autores podem facilmente deixar descrito no conteúdo quais os limites de uso do mesmo, através de uma iconografia específica.

Além de regras claras, a web precisa de uma Justiça mais célere, na verdade, de um Judiciário totalmente digital também. Mas, mesmo com tudo isso ocorrendo, não seremos capazes de garantir uma internet mais segura e saudável para todos sem educação.

O próprio Judiciário poderia tomar mais proveito do uso de ferramentas tecnológicas que permitissem a análise de casos similares e todas as decisões já tomadas, como se fosse um Juiz digital que tem uma base de dados de precedentes e assim pode servir de orientação sobre como decidir um conflito.

Isso é importante porque o Juiz, como um ser humano, possui suas próprias convicções e dependendo da situação pode não estar a par dos princípios que devam reger a análise de uma situação concreta, ainda mais quando envolve os meios digitais, que são algo muito novo e ainda sem muitas referências.

Michael Sandel, professor de filosofia de Harvard, em sua obra sobre Justiça, traz justamente a provocação "o que é fazer a coisa certa"? Independente de eventual punição, será que aprendemos a tomar decisões baseadas em um conjunto único de valores que definem e distinguem a decisão certa da decisão errada?

Apenas para ilustrar, já tratamos do problema da falsa identidade na internet. Mas será que um pai poderia se fazer passar pela filha menor de idade para dialogar com um suposto amigo digital desta a fim de gerar flagrante de assédio ou de pedofilia?

Como ficaria então a aplicação do instituto da legítima defesa, previsto no artigo 25 do Código Penal Brasileiro, em uma situação na internet? Até onde podemos ir sem que uma medida de proteção se transforme também numa infração?

Entende-se por legítima defesa quem, usando moderadamente dos meios necessários, repele injusta agressão, atual ou iminente, a direito seu ou de outrem. Portanto, a legítima defesa ocorre quando seu autor pratica um fato típico, previsto em lei como crime, para repelir a injusta agressão de outrem a um bem jurídico seu ou de terceiros.

O futuro da regulamentação da Internet, como local onde exercemos nossa vida digital, depende diretamente do alinhamento de um rol de princípios uniformes que devem estar legitimados e ser de conhecimento de todos os seus participantes.

A partir desta base de princípios éticos é que se pode construir qualquer ordenamento legal, onde a regulamentação é apenas um meio de instrumentalizar a sociedade para que se faça cumprir o que tiver ficado combinado.

Estamos enfrentando já o dilema trazido pelas novas tecnologias de comunicação que permitem aumentar segurança mas que ferem as garantias de privacidade, vide as acusações entre diversos países sobre a espionagem digital justificada e legitimada com base na necessidade de se combater o terrorismo, mas que pode ser facilmente extrapolada para atender outros interesses escusos.

A Internet nos tornou uma aldeia global, agora precisamos construir um novo modelo integrado de autoridade que possa representar todas as culturas, povos e cidadãos que já convivem neste novo ambiente digital.

Por certo, um cadastro único de internauta seria muito útil. Mas imagine o poder deste banco de dados que pudesse associar quem é cada um e o que está fazendo na web? Quem poderia gerenciá-lo? Quais seriam os limites?

Como fazer uso do Big Data de forma ética e legal? O uso das informações dos indivíduos que estão esparsas de forma estruturada ou não em meios digitais e bancos de dados é justamente a pauta de leis e projetos de lei em diversos países, inclusive no Brasil.

A Internet avançou muito do ponto de vista econômico e social, em tudo aquilo que pode ser realizado por auto-regulamentação do próprio mercado, pela iniciativa privada. Mas a grande quebra de paradigma envolve justamente a faceta pública da mesma, que vai desde as discussões de arrecadação de tributos até de implementação de poder de polícia.

Por certo, se a privacidade é um conceito que está em transformação, o mesmo podemos dizer sobre soberania. Como redefinir este instituto em um momento do desenvolvimento tecnológico da sociedade humana em que há livre circulação de pessoas e bens através da Internet?

Como garantir acesso para todos? A inclusão digital delimita a separação entre os desenvolvidos e os marginalizados na Sociedade do Conhecimento. Mas além de incluir, temos que capacitar, educar, investir em sustentabilidade até para evitar o tão assustador apagão digital.

A Nova Ordem Digital exige um Estado bem mais articulado, que compreenda o seu real papel em equilibrar as forças que devem garantir o crescimento com fornecimento suficiente de recursos essenciais quais sejam: Energia, Telecomunicações e Tecnologia. E nesta agenda pública, o Brasil está atrasado.

Além da infraestrutura, cabe a este Estado Digital desenhar uma arquitetura jurídica internacional que permita a proteção de seus cidadãos e dos dados destes quando estiverem conectados, bem como também atualizar a grade de ensino para melhor prepará-los para esta realidade competitiva e globalizada.

Um Estado que saiba tomar proveito das ferramentas atuais de inteligência coletiva e de colaboração digital para aumentar a riqueza bem como a sua distribuição. Se estamos na Sociedade do Conhecimento, a produção criativa e a propriedade intelectual tendem a crescer de valor como insumos econômicos.

Concluindo, nesta jornada rumo ao próximo estágio da Internet, que passa a exigir uma dimensão política-jurídica mais global, teremos que enfrentar todas estas questões fundamentais para garantir segurança e bem estar social-digital, que vão desde a criação de um modelo único de identidade não repudiável, que pode ser da autenticação biométrica ou outra tecnologia que se invente até o que fazer com esta nova versão de criminoso muito mais tecnológico.

Dra. Patricia Peck Pinheiro é advogada especialista em Direito Digital, formada pela Universidade de São Paulo (Twitter:@patriciapeckadv), é sócia fundadora do escritório Patricia Peck Pinheiro Advogados (www.pppadvogados.com.br), da empresa de cursos Patricia Peck Pinheiro Treinamentos, do Instituto ISTART de Ética e Segurança Digital que conduz o Movimento Família mais Segura na Internet (www.istart.org.br) e apresenta o talk-show "É Legal" (www.youtube.com/programaelegal).