



***Primeiros questionamentos sobre a
Lei Brasileira da Internet
(Lei 12.965/2014)***

No final de junho de 2014 passará a vigor norma federal que regulamenta os 'princípios, garantias, direitos e deveres' para o uso da Internet no Brasil. A norma, publicada em 23 de abril, veio tarde relativamente ao trato legal da matéria ao redor do mundo, bem como a atual importância da rede. Mas antes de adentrar propriamente em algumas determinações da lei, é preciso colocar sobre a mesa pontos importantes para refletirmos acerca do rumo que o mundo anda tomando no que se refere a Internet. O primeiro ponto tem a ver com um fato recente noticiado como uma seríssima falha de segurança no *SSL*, denominada de *HeartBleed*, segundo a qual a informação tunelada nas páginas *https* não estaria protegida devidamente. Esta falha de segurança na comunicação de dados, em termos práticos, pode ter exposto milhões de dados, de milhões de pessoas, ao redor do planeta, dados estes coletados, tratados e armazenados, por exemplo, pelos EUA,

como vem sendo amplamente noticiado na mídia, desde o caso *Snowden* até o programa *PRISMA*. Estamos a apontar, então, algo relativo a intimidade e privacidade das pessoas. Mas que intimidade e privacidade? As pessoas, no mundo contemporâneo onde a todo instante somos registrados, taxados e quantificados, ainda têm a possibilidade do direito fundamental ao que é da ordem do personalíssimo? É possível a privacidade no mundo contemporâneo? Outro dia foi noticiada a discussão de implantação de GPS de fábrica nos carros à disposição no mercado automobilístico brasileiro. Ou seja, a possibilidade do Estado saber as rotas que cada cidadão motorizado faz, além, é claro, daquela possibilidade defendida de que isto poderia agregar em nossa segurança. De igual modo, o sistema que viabiliza o crédito tributário concedido quando informamos nosso CPF em uma simples compra de alimentos no supermercado tem potencial tanto para informar ao Estado sobre atos ordinários da vida de cada um (monitorando e quantificando o já coisificado humano), quanto tem potencial para dar 'pão e circo' – quero dizer, 'crédito tributário'. E os exemplos se multiplicam Brasil e mundo afora, passando, em nosso caso, pelo *SPED*



BRNews | Tecnologia, Direito & Política: Internet

e o processo digital, este ainda seriamente falho em alguns pontos. E aqui preciso abrir um parêntese e alertar sobre uma experiência minha enquanto advogado contencioso: descobri que uma folha de um processo judicial que corre na Justiça Estadual Bandeirante pode ser trocada por outra, como de fato o foi, por um servidor do Cartório, sem que se saiba o que havia na folha anterior – ou seja, total insegurança jurídica. Estou aqui a falar sobre como o Estado trata a tecnologia a seu favor e, muitas vezes, em desfavor do cidadão. O mesmo, é claro, ocorre com as grandes empresas, que processam milhares e milhares de dados a todo instante. Os Bancos sabem o que seu consumidor adquire quando passa seu cartão de crédito. Os proprietários das redes sociais e dos sites sabem até as preferências sexuais de seus visitantes. E o cidadão comum? Sabe o cidadão comum de todos estes exemplos bárbaros? E se sabe, dá importância? Assim, a questão não se resume apenas a técnica de ser possível cada vez mais manter, ou não, um dado sob sigilo absoluto. Nossa reflexão passa, primeiro, pela questão de opção que está sendo feita pela sociedade, por meio dos assim intitulados representantes do povo,

acerca da exposição ou não do que a moral dos tempos considera como íntimo. Pois bem, colocadas estas provocações iniciais sobre a mesa, com o intuito de fazê-lo refletir, caro leitor, adentremos um pouco na novel Lei 12.965/2014. Os políticos determinaram, por um lado, que deve haver registro de conexão e acesso a aplicações de Internet (Art. 5º, incisos III, VI e VIII) e, por outro lado, os representantes do povo estabeleceram como lei que deve haver a exclusão definitiva de dados pessoais quando do término da relação contratual (Art. 7º, inciso X), em respeito a intimidade e vida privada (Art. 8º e 10º), sob pena de as empresas pagarem até 10% do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos. Ora senhores e senhoras, a lei diz que futuro decreto regulamentará o procedimento para apuração de infrações sobre guarda e disponibilização dos *logs*, mas, de um ponto de vista prático, é possível fiscalizar a exclusão e manipulação de dados? A não ser que haja denúncia, parece improvável demais rastrear se uma empresa de TI vendeu seu banco de dados de clientes para outra. E se isto acontecesse, seria necessariamente uma infração? Ou seria



BRNews | Tecnologia, Direito & Política: Internet

parte de um processo de fusão e aquisição? Outro ponto importante, que pode gerar questionamento com múltiplas respostas pelo Poder Judiciário nas soluções às futuras demandas, diz respeito ao grau de consentimento esclarecido por parte do consumidor acerca do que será feito com seus dados. E na prática? Será possível saber o que será feito? Quando vou a um Banco que me solicita um cadastro biométrico, como saberei para quais finalidades serão usadas minhas digitais? Seria lícito transmitir automaticamente estas informações para o TSE, para fins de eleição e identificação mais precisa do eleitor? – o que, frise-se, não significa, de modo algum, eleição mais segura. Estas transferências e tratamentos de dados, determinadas de cima para baixo, parecem ser uma moda que já pegou nos EUA quando consideramos que em 2013 ocorreu aprovação da Câmara dos Representantes dos EUA do *Cybersecurity Bill*, projeto legislativo que permite empresas partilharem dados pessoais de clientes com outras empresas e o governo norte-americano, mesmo que os contratos já firmados destas empresas expressem o contrário. Como se nota, é preciso fortalecer a proteção de direitos fundamentais de

privacidade no Brasil e no mundo, mas, ao mesmo tempo, o poder de imposição do Estado e dos grandes grupos econômicos é inegavelmente efetivo ante a ausência de esclarecimento das pessoas sobre as consequências e manipulações advindas da super-exposição de seus dados. Ausência de esclarecimento significa ausência de Educação sobre as consequências de certos atos. Por fim, após alguns questionamentos que acredito serem capazes de nos fazer começar a refletir mais profundamente sobre a Internet e os seus atuais usos, torna-se fulcral registrar uma situação interessante que faz com que o extremo monitoramento se torne pernicioso e prejudicial. Projetos como o *TOR*, que visam a não identificação, que visam não deixar rastros, pelos navegantes, justificam-se, por exemplo, como meios de se proteger em regimes totalitários, mesmo naquelas ditaduras que são silenciosamente autoritárias e controladoras, as quais parecem ter ganho musculatura nos últimos 15 anos. Neste sentido, o anonimato serviria para a proteção do ser humano. E o que dizer de uma situação em que cidadãos desejem verificar dados econômicos públicos, por uma razão de transparência e fiscalização, mas não



BRNews | Tecnologia, Direito & Política: Internet

querem ser identificados, pois usarão tais dados para apontar um esquema de corrupção? A investigação e a denúncia, na Internet, não deveriam poder ser anônimas? Neste sentido, deveria o site da Polícia registrar dados como IP? Como se vê, existe a impossibilidade de se exigir tamanho controle de identificação em muitas situações cuja defesa é moral e juridicamente legítima. Ou seja, é preciso compreender a novel lei 12.965/2014 à luz dos casos concretos, afastando sua aplicação, inclusive, quando necessário, bem como, é preciso um constante acompanhamento dos efeitos que serão gerados, de modo a aperfeiçoar a norma, depurando-a com a realidade. Como as sementes, as leis novas ainda não amadureceram em flores e frutos e, assim, escondem seu potencial, ou sua desgraça, até que o tempo os revele. *Alea jacta est.*

por Rafael De Conti | Advogado

www.decontilaw.com.br

