Seus Dados São Você: Porque o Brasil Precisa de uma lei de proteção de dados pessoais
Proponente: Coalizão Direitos na Rede
Co-proponente: CTS
Relatoria: Bia Barbosa (Intervozes)

Participantes/debatedores: Ana Paula Bialer (Brasscom – setor empresarial); Miriam Wimmer (MCTIC – governo); Lucas Teixeira (Coding Rights – terceiro setor); Renato Leite Monteiro (Mackenzie – setor acadêmico); Danilo Doneda (UERJ – setor acadêmico)
Moderação: Flávia Lefèvre (Proteste)

A abertura do painel, feita pela moderadora Flávia Lefèvre, recuperou o histórico de elaboração do Projeto de Lei 5276/16, de proteção de dados pessoais, e sua tramitação na Câmara dos Deputados, onde se encontra a espera do relatório da Comissão Especial de Dados Pessoais, a ser elaborado pelo deputado federal Orlando Silva (PCdoB/SP). Enquanto isso, no Senado Federal, tramita o PLS 330/13, de autoria do senador Antônio Carlos Valadares. Recentemente, um substitutivo apresentado pelo senador Ricardo Ferraço (PSDB/ES), relator do PLS na Comissão de Assuntos Econômicos do Senado, coloca em riscos alguns direitos importantes desse projeto. Em apoio à existência de uma lei que proteja nossos dados, a Coalizão Direitos na Rede lançou, em setembro, a campanha "Seus Dados São Você" e propôs a realização deste painel no Fórum da Internet.

Em seguida, cada um dos debatedores participantes apresentou suas reflexões sobre o tema, sintetizadas abaixo.

Ana Paula Bialer – BRASSCOM
Acredita que o Brasil já avançou bastante no debate sobre a necessidade de uma lei de proteção de dados pessoais, e que agora estamos num momento de buscarmos um mínimo denominador comum entre os diferentes setores neste processo. Já temos muitos princípios e conceitos em comum, mas este debate não deve ser feito apenas da ótica da proteção dos direitos individuais (que é fundamental enquanto baliza), e sim de todo o ecossistema envolvido, dos pequenos e grandes empreendedores que estão colhendo dados para inovar, trazer desenvolvimento econômico, inclusão social e digital por meio deste trabalho. Para ela, uma lei deve proteger a todos, incluindo aquele que coleta e trata dados, para que faça isso respeitando a expectativa e os direitos do titular dos dados. Hoje vivemos um cenário de inteligência artificial, de Internet das Coisas, de bigdata e onde se coleta muito dado, e mal começamos a tirar benefícios disso. Somente 5% dos dados hoje coletados são trabalhados e se cria soluções em cima deles. E as inovações não são focadas somente no benefício econômico de quem explora, mas de todos nós. Por exemplo: uso de bigdata para monitorar a epidemia do zika vírus; para detecção de câncer em tempo inferior; para a agricultura de precisão, com queda no desperdício de alimentos e aproveitamento do solo; etc. Será que é preciso tantas amarras então para a coleta de dados? Em 2020, segundo a Cisco, teremos 50 bilhões de equipamentos conectados em todo o mundo. Nem todos eles terão interface para a manifestação do consentimento dos usuários. Como faremos isso então neste contexto? Não é possível utilizar referências diferentes das que temos hoje, para garantir que os direitos dos titulares dos dados sejam observados, mas que essa observância não inviabilize o processo de inovação? Até o momento, no Brasil, a discussão foi muito pautada no modelo europeu. Um modelo importante para a proteção dos direitos dos cidadãos na rede, mas com as amarras que ela carrega, não faz sentido importar os mesmos conceitos. Temos uma oportunidade única de evoluir na legislação que existe na Europa, procurando inspiração em outros modelos, pois há vários países com boas ideias. Então nos parece importante honrar os princípios mas inovar nos conceitos, trazendo uma abordagem mais baseada no risco: coletar dados não é necessariamente ruim, o problema é usar isso para prejudicar seu titular. Não conseguimos rever a definição de dados pessoais e de dados anônimos para considerar os diferentes tons de cinza que existem no debate? Talvez não precise ter um escopo tão restritivo

de proteção, como posto hoje no PL 5276. E aí calibrar para trazer a responsabilização para aquele que trata dos dados; caso não honre com finalidade da coleta, a expectativa do titular e caso não zele pela guarda, seja responsabilizado caso aja de maneira negligente. Para o Brasil se destacar neste contexto da economia digital, precisamos de uma nova abordagem. Um ecossistema digital só funciona na medida em que todos confiem neste ecossistema: que as empresas tratarão os dados de maneira íntegra e responderão caso não o façam. Por isso, ter um incentivo a medidas de corregulação e de privacy by design parece mais efetivo e indutor do desenvolvimento do que ter conceitos rígidos na lei.

Miriam Wimmer – MCTIC
Iniciou sua fala afirmando que o Ministério atualmente tem sua política voltada para a inovação, para o desenvolvimento de modelos de negócio e a transformação digital. Na Sepin, o esforço tem sido o de construir uma estratégia para lidar com a transformação digital que acontece tanto no âmbito do governo como na economia, como a questão da IoT, do crescimento das plataformas digitais, etc. O governo quer compreender essa transformação e criar um ambiente que permita captar os benefícios dessa transformação. O MCTIC, em parceria com 9 órgãos de governo e em diálogo com 40 entes públicos, trabalhou então para colocar em consulta público o documento "Estratégia Brasileira para a Transformação Digital", que identifica, a partir de 9 eixos (infraestrutura, dimenção internacional, educação, etc), um diagnóstico de onde estamos, uma visão de onde queremos chegar e identifica ações estratégicas para chegar até lá. É um esforço harmônico com discussões que acontecem em outros países (em fóruns como BRICs, Cepal e G20), apoiado em indicadores de produtividade, inclusão, resultados na educação – e há forte relação positiva entre países que adotam a tecnologia digital de maneira mais intensa nos seus processos produtivos e ações de governo com indicadores como PIB, renda e competitividade. O Brasil, infelizmente, está longe da dianteira desses rankings digitais; pelo contrário, temos uma tendência de queda neste sentido. E um dos eixos que o MCTIC trabalhou neste documento é o de confiança, que dialoga não apenas como temas como combate a crimes cibernéticos mas também com a existência de um ambiente que respeite os direitos fundamentais, do consumidor e ligados à privacidade. Neste documento, então, o governo buscou compreender o papel dos dados nessa nova economia. Alguns relatórios apontam o crescimento do fluxo de dados nos últimos anos na ordem de 40 vezes. Isso se associa a um desenvolvimento tecnológico muito intenso. Então, ao reconhecer que dados são um elemento estratégico para o crescimento econômico do país, há uma necessidade de se atribuir segurança jurídica quanto à forma de coleta, tratamento e armazenamento desses dados – tanto para as empresas quanto para o cidadão, que é o titular de seus dados. Os projetos de lei que estão no Congresso devem buscar um ponto delicado de equilíbrio entre a proteção de direitos e a inovação e viabilização de modelos de negócio característicos dessa economia digital, da qual o Brasil ainda participa de maneira periférica. É importante haver um engajamento da indústria na viabilização dessa proteção de dados, porque mecanismos que confiam plenamente na ideia de consentimento do cidadão são frágeis. A fadiga do consentimento já é conhecida. Então a aplicação de privacidade por design, na própria formulação dos aplicativos e dispositivos, é pré-requisito para o sucesso da lei. Há uma forte assimetria de informações entre o poder público e o setor empresarial, então o incentivo a códigos de conduta empresariais debatidos com o poder público, boas práticas internacionais, etc parecem ser mecanismos muito importantes para a segurança das empresas e usuários. O MCTIC acha importante a aprovação de uma lei neste sentido e a identificação/criação de uma instância para tratar do tema. Uma legislação mais principiológica pode funcionar se houver a clareza de quem vai interpretá-la para não cairmos numa situação de judicialização intensa deste tema. Importante então aprofundar este debate para, no curto prazo, termos uma legislação adequada e bem calibrada.

Lucas Teixeira – Coding Rights
Buscou fazer uma fala para traduzir e explicar para o público geral o que é este ambiente de troca intensa de dados que estamos vivenciando. Uma das iniciativas da Coding Rights para chamar a

atenção para o tema é o projeto “Chupa Dados” (www.chupadados.com), que traz narrativas jornalísticas sobre temas como aplicativos de menstrução para mostrar que tipos de dados são coletados; como as crianças estão usando o Youtube como plataforma de entretenimento e como isso as submente a venda de produtos; de plataformas de serviços “gratuitos”, que se financiam coletando dados da sua vida. Chamou atenção para a rede de empresas que tem coletado dados que podem parecer não relevantes (como fazer um cadastro numa farmácia) e como, na troca desses dados, tem desenvolvido perfis de consumo, entretenimento, comportamento e saúde dos cidadãos. E contou como a campanha Seus Dados São Você tem trabalhado para alertar os cidadãos sobre esta questão e também defender, do ponto de vista jurídico, uma lei que proteja nossos direitos e nos projeta do “Chupa Dados”, que tem definido cada vez o que vamos consumir na internet, qual o valor de um seguro que nos será oferecido, que opções nos serão apresentadas. É uma luta pela autodeterminação informativa, para que estejamos no controle das nossas informações, sabendo o valor que elas tem e tendo condições de saber escolher e ter amparo legal para fazer o direito valer nessas escolhas. Num contexto de eleições, por exemplo, empresas como a Cambridge Analytica trabalham coletando dados, comprando dados de databrokers e montando perfis para direcionar propaganda política de acordo com o seu perfil psicológico. Essa empresa foi fundamental na vitória do Donald Trump nos EUA e do Brexit no Reino Unido. A Coalizão Direitos na Rede defende então uma lei forte de proteção de dados pessoais, com definições importantes como dados sensíveis e anonimização (um estudo mostra que somente através da data de nascimento, do gênero e do CEP mostrou que é possível identificar 87% dos habitantes dos Estados Unidos; e que são necessários somente 33 bits de informação para identificar uma pessoa).

Renato Leite Monteiro – Mackenzie
Ponderou que não é preciso ter um posicionamento binário e sim harmônico para construir uma regulamentação da proteção de dados que seja forte. O conceito de dado pessoal, neste sentido, deve ser compreendido como uma informação que é relacionada direta ou indiretamente a uma pessoa natural. Não é só uma informação que identifica uma pessoa diretamente. Nos PLs, há conceitos diferentes que determinam quando a lei deverá ou não ser aplicada. Acontece que hoje, devido ao processamento, quase todos os dados podem ser considerados dados pessoais. Mas isso não necessariamente representará um entrave à inovação. Trabalhar com a ideia de risco e de confiança nas empresas pode ser interessante. Mas trabalhar só no eixo da confiança é complicado diante de um cenário de escândalos de vazamento, inclusive em empresas que tinham como atuação core processar e armazenar dados – e que tem feito até os EUA repensar o seu modelo regulatório, pensando numa lei federal para proteger dados pessoais. A própria questão da privacy by design requer alguma intervenção para garantir que ela aconteça, não apenas mediante confiança nas empresas. Os PLs que estão em discussão no Congresso tratam do risco, como a previsão, no PL 5276/16, da apresentação de relatórios de impacto, que são impactos de análise de risco, para a autoridade reguladora, justamente para identificar se aquela metodologia de tratamento de dados traz risco ou não para o titular dos dados. Então, sim, a ideia de risco já está em debate, mas isso não deve caber só às empresas. Nos EUA, a FCC aplica multas da ordem de 30 milhões de dólares para casos de dano. E no Brasil a pena máxima prevista no PLS 330 é de R$ 93 mil reais. A GDPDR (Europa) preve multa de até 4% do faturamento da empresa, servindo como um incentivo para melhores práticas. Outra ideia importante é a de consentimento. Realmente a fadiga do consentimento existe (todo mundo dar o “sim” sem ler as políticas de privacidade dos aplicativos), mas isso não significa que tenhamos que abolir o consentimento. Ele continua sendo o eixo principal para autodeterminação informacional. Temos, inclusive, que aproveitar momentos como o do debate da Internet das Coisas para discutir como o consentimento deve ser feito – e não aboli-lo. O PL 5276 entende, por exemplo, que o consentimento é apenas uma das 9 bases legais para o processamento de dados pessoais. Outra é o legítimo interesse, que também não pode ser um cheque em branco, que permita que empresas e governos tratem dados pessoais para quaisquer finalidades. Como previsto na regulação européia, o legítimo interesse obriga um teste de proporcionalidade e adequação muito forte em favor do titular. Temos, então, uma grande

oportunidade para pensar um modelo regulatório que seja adequado, mas que não seja somente permissivo e construído com base em argumentos de inovação. Podemos ter uma lei, inclusive, que seja modulada, como faz o PL 5276, que permite que uma eventual autoridade de proteção de dados pessoais reveja regras para pequenas empresas. O que estamos discutindo hoje é a necessidade de segurança jurídica, para garantir a inovação e o desenvolvimento econômico sem mitigar qualquer direito ou liberdade individual.

Danilo Doneda – UERJ

Iniciou sua fala recuperando um pouco do histórico do Brasil neste tema, como um dos poucos países que não possuem uma lei geral de proteção de dados, ao contrário de outros 121 no mundo todo. Hoje temos um marco regulatório que cobre alguns aspectos da privacidade, mas sem uma articulação única e que faça sentido e proporcione segurança para o cidadão sobre quais são seus direitos, a quem recorrer, o que pode de fato ser feito em relação a seus dados. E isso é ruim pra todo mundo, para quem trata dados – porque não sabe os limites e onde pode ir –, e para os usuários. Normas como o CDC e o Marco Civil da Internet abordam a proteção de dados pessoais de forma incidental, mas fazem isso de forma parcial e setorial. A grande novidade que uma lei de proteção de dados pessoais traz é que esta é a única forma de se garantir direitos fundamentais do cidadão na sociedade da informação. A medida em que a interação com o Estado e com as empresas passa pela troca de dados pessoais, qualquer alteração, ruído ou exercício de poder neste fluxo de informações pode representar danos a garantias fundamentais de qualquer ordem. Não se trata de proteção só da privacidade, embora ela esteja contida na ideia de proteção de dados pessoais, mas também de direitos como a saúde e à própria vida. Então não tratar da proteção de dados é abdicar de atualizar direitos humanos para toda uma população. Outro elemento importante para o debate é entender os dados como uma projeção da pessoa e da sua personalidade – daí o nome da campanha "Seus Dados São Você". Tanto que, se não for assim, esse dado deixa de ser útil – representam uma entidade não existente. Os dados são projeções da nossa personalidade, são o nosso corpo eletrônico que deve ser protegido por um habeas data. Então uma pessoa, além de ter direito à proteção dos seus dados, se insere na dinâmica social e na economia da informação através do compartilhamento desses dados. Então é errado pensar que esses dados são de livre tratamento. É fundamental fornecer transparência, controle e respeitar o cidadão no sentido de que suas garantias serão tuteladas num ecossistema no qual seus dados devem ser tratados de acordo com o seu interesse e a sua vontade. Neste sentido, ao se retirar o consentimento de um marco de proteção de dados pessoais, algo tem que ir no seu lugar. Um enfoque no sentido do risco pode ser mais factível, porém regular através do risco pressupõe regular com base na responsabilidade objetiva. Como saber, por exemplo, se você teve um emprego negado em função de um tratamento abusivo dos seus dados? Então a falta de medidas sansionatórias para o uso abusivo de dados pessoais é fatal. Então, tirando o consentimento, algo tem que vir no lugar. O PL 5276 é bastante flexível em relação ao consentimento, que é mais flexível do que o próprio Marco Civil da Internet, que pretende-se moderno e indutor da inovação, e pressupõe o consentimento expresso – que não está no PL 5276. O consentimento então não é uma trincheira. Ele é uma forma de funcionalizar a ideia de que o cidadão tem que ter controle e domínio sobre seus dados e o que é feito com eles. Se houver outro instrumento pra isso, que bom. Outro tema fundamental é a questão da autoridade reguladora. Dessas 121 leis de proteção no mundo, 110 outorgam a algum órgão público a função de ser uma autoridade de proteção de dados, para zelar pela aplicação da lei. Essa autoridade é necessaria porque a regulação da proteção de dados é muito dinâmica, tem que ser constantemente atualizada; para reduzir a assimetria informacional das empresas em relação ao cidadão; para a regulação do mercado e para o Estado reconhecer melhores práticas. Então uma autoridade única, independente e autônoma é fundamental. A unicidade da regulação é importante tanto para o cidadão saber que direitos tem quanto para o próprio fluxo de informações no mercado. Imagine cada setor obedecendo a regras diferentes… isso não funciona na economia da informação. Então é importante ter muito cuidado para não preservar um sistema de privilégios de alguns setores, como algumas

propostas com patrocinadores importantes vem sendo apresentadas. Destacou, por fim, a questão da assimetria informacional, não apenas entre empresas e cidadãos, mas também entre o mercado e o poder público, citando como exemplo países em que a pesquisa na área de saúde é feita substancialmente por grandes empresas (que não fornecem acesso aos dados para o poder público para fins de políticas públicas) ou do sistema de crédito pelos bancos. No caso dos cidadãos, se ele não tiver instrumentos jurídicos para equilibrar essa assimetria, a informatização da nossa vida vai nos relegar a um lugar de passageiros da nossa autonomia perdida.

Ao longo da apresentação dos debatedores, a moderadora Flávia Lefèvre fez alguns comentários:

Lembrou que o receio da sociedade é que, sem a observância dos princípios de uma maneira mais rígida, dados sensíveis possam ser usados de maneira abusiva – algo que já vei acontecendo em países em que a legislação é menos flexível. E que por isso a sociedade civil tem reforçado esses princípios.

Lembrou que a sociedade civil tem se preocupado com algumas declarações de membros do governo que tem criticado a definição de consentimento como prevista no artigo 7º do Marco Civil da Internet, que deve ser expresso e informado. Para termos um ambiente de confiança, o consentimento deve ser uma premissa.

Por fim, dentro da preocupação sobre segurança jurídica, informou que nenhum dos PLs traz a instituição de um órgão com competências reguladoras e fiscalizadoras para garantir que os direitos que venham a ser estabelecidos por uma lei tenham eficácia. Porque, senão, diante de conflitos que surgirão, essas questões irão parar no Poder Judiciário e o grau de incerteza e insegurança cresce para todos os envolvidos. Por isso a criação de uma autoridade reguladora para a proteção de dados pessoais é um dos pontos de consenso entre empresas e organizações da sociedade civil.

Debates com o público

Foram levantadas questões como a possibilidade de um caráter multissetorial para esta autoridade de proteção de dados pessoais; sobre o risco do Brasil ser alvo de empresas como a Cambridge Analytica e qual o papel do TSE neste contexto; sobre a relação de um projeto de lei de proteção de dados pessoais com um projeto de nação para o Brasil; sobre como melhorar os PLs ainda em tramitação no Congresso, incluindo questões como incentivos para práticas de accountability nas empresas no texto das leis; sobre a opacidade das empresas x a transparência que é exigida do cidadão, num contexto de total assimetria; sobre o direito do cidadão de ter acesso a banco de dados que nos encaixam em perfis determinados; sobre a possibilidade de uma regulação forte também trazer externalidades positivas; sobre o movimento de municipalização de projetos de proteção de dados pessoais, diante de um cenário de desenvolvimento de “cidades inteligentes”; e sobre os mitos na relação privacidade x segurança e privacidade x inovação.