Centre for Information Policy Leadership (CIPL) e Centro de Direito, Internet e Sociedade of Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (CEDIS-IDP)

Segundo Diálogo Global de Proteção de Dados

Abertura do Primeiro Dia – Visitando os últimos seis anos e olhando o futuro da proteção de dados no Brasil e no mundo

Estamos vivendo a quarta revolução industrial e, por conta da pandemia do COVID-19, esse movimento de avanço e inovação foi impulsionado. Segundo **BOJANA BELLAMY**, Presidente do CIPL, consequências disso são o aumento do fluxo internacional de dados e o uso de sistemas de Inteligência Artificial (IA). A utilização de IA depende da possibilidade de acessar dados, tratá-los e ter *pools* de informações para finalidades específicas. Nesse sentido, nos últimos seis anos, estamos vivendo algumas tensões que devem ser analisadas: é a era pós Regulamento Geral de Proteção de Dados (RGPD, norma europeia sobre proteção de dados), que foi um farol para muitos países na forma de regular o tratamento de informações pessoais; os fluxos livres de dados, em que governos estão percebendo a importância dos dados e utilizando essas informações para fins econômicos e sociais, ao mesmo tempo há preocupação sobre transferência e soberania de dados; por fim, o uso responsável de dados, em vista de uma responsabilidade corporativa em relação a dados, tema que passou a ser discutido pelos conselhos das empresas.

Para **LAURA SCHERTEL**, Diretora do CEDIS, o ano de 2020 foi determinante no Brasil. Nesse ano a LGPD entrou em vigor, a ANPD foi instaurada e o Supremo Tribunal Federal decidiu pela existência de um direito fundamental à proteção de dados**.** Por isso, precisamos pensar sobre a forma de aplicação da Lei de modo a gerar confiança nas relações entre empresas, titulares de dados e Estado. Assim, alguns dos elementos desafiadores estão relacionados ao fato de a LGPD regular o fluxo de informação e a natureza do objeto regulado ser própria e específica. Ainda, é natural que o dado flua, por isso o debate deve ser considerado também a nível internacional. Dessa forma, a parceria do CEDIS-IDP e o CIPL é fundamental para o debate técnico e multissetorial a fim de tornar efetiva a interpretação da LGPD, além de considerar as peculiaridades de cada país, como os desafios de uma regulação institucional.

Keynote 1 - Agenda e prioridades regulatórias da ANPD

WALDEMAR GONÇALVES ORTUNHO JR, Diretor-Presidente da Autoridade Nacional de Proteção de Dados do Brasil (ANPD), destacou ser fundamental que o tema da proteção de dados seja fomentado em eventos, tendo em vista a criação recente da ANPD e os desafios que a Autoridade está enfrentando no momento. Por isso, é necessária a promoção de um debate sobre o impacto da proteção de dados na vida cotidiana para os cidadãos brasileiros. Apesar dos desafios de iniciar uma autoridade e ainda possuir um quadro de pessoal reduzido a 36 servidores, o órgão já realizou ações relevantes, como a elaboração do Regimento Interno da ANPD[1] e uma Agenda Regulatória[2] para garantir celeridade aos processos. Isso foi possível a partir da análise de experiências de outros órgãos nacionais e internacionais, de forma a mapear os procedimentos que poderiam ser adaptados e replicados. Assim, será possível construir uma estrutura de autoridade mais robusta para o país, que é extenso e peculiar. Além disso será necessário organizar planejamentos futuros, como a possibilidade de revisão de organização interna e quadro de pessoal da ANPD. Outra dificuldade é a capacitação de pessoal, mas essa atividade já está em desenvolvimento, inclusive com a participação do corpo técnico da Autoridade em um curso específico para os servidores oferecido pela Comissão Europeia[3].

Ainda, há o desafio de normatização complementar, por isso foi feito um mapeamento das atividades e foram definidas as prioridades da Autoridade para formar uma Agenda Regulatória robusta. Isso não quer dizer que outras pautas não serão enfrentadas pela ANPD, já que a realidade traz desafios que serão estudados de acordo com as demandas concretas, como a questão referente à transferência internacional de dados. A construção de regulação irá ocorrer por meio de audiências públicas e tomadas de subsídios. Essa metodologia está sendo seguida no caso da análise de temas como notificação de incidentes de segurança, além de tratamento diferenciado para pequenas e médias empresas. Outra atuação da ANPD foi sobre a política de privacidade do WhatsApp, em que a ANPD, em colaboração com outros órgãos, teve oportunidade de apresentar nota sobre a atualização da política de privacidade. Por fim, foi ressaltado que a ANPD acredita que a prioridade é criar cultura de proteção de dados,

---

[1] Disponível em: < https://www.in.gov.br/en/web/dou/-/portaria-n-1-de-8-de-marco-de-2021-307463618 >. Acesso em 15 de junho de 2021.
[2] Disponível em: < https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313 >. Acesso em 15 de junho de 2021.
[3] Disponível em: < https://www.gov.br/anpd/pt-br/assuntos/noticias/servidores-da-anpd-concluem-capacitacao-pela-universidade-de-maastricht-no-ambito-do-projeto-data-protection-academy-da-comissao-europeia >. Acesso em 15 de junho de 2021.

conscientizar a população e destacar a funcionalidade de boas práticas para as empresas, só assim a LGPD será aplicada de forma responsável e transparente.

Keynote 2 - Perspectivas britânicas e globais sobre proteção de dados

Na perspectiva de **SIMON MCDOUGALL**, Diretor Executivo do *Information Commissioner's Office* (ICO), as autoridades de proteção de dados já encontravam diversos desafios, porém a COVID-19 acelerou a urgência dessas dificuldades e criou novos problemas. Alguns exemplos de inovação foram vistos no uso de dados de saúde para acelerar programas de vacinação e diminuir a transmissão do vírus além dos casos de uso de passaportes de vacinas e aplicativos de *contact tracing*. Nesse cenário, foram percebidos desequilíbrios de poder no tema de proteção de dados pessoais, mas Simon sinalizou que a confiança é um diferencial para a observância da proteção de dados dos cidadãos.

Agora fica evidente como os dados estão inseridos na nossa vida cotidiana, além de a quantidade de dados produzidos ser cada vez maior. Com a pandemia, essa afirmação passou a ser senso comum e outros *stakeholders* se interessaram por esse assunto. Para as autoridades de proteção de dados, isso significa que a linha de frente do trabalho é ampla sobre diferentes questões que devem ser enfrentadas. Por isso, deve-se focar nos desenhos de prioridades, tendo em vista que existe uma dificuldade de manter essa pauta diante das novas demandas criadas todos os dias. Ainda, deve-se se atentar para a gestão de riscos, com a perspectiva multidisciplinar nesse cenário complexo, e com acesso a conhecimentos para além da legislação. Ainda, é preciso ter princípios sólidos, acesso a outros atores e consciência sobre o contexto social.

Para a ICO, a privacidade é direito fundamental, mas não absoluto; a COVID-19 deixou isso evidente. Nesse contexto, alguns desafios foram postos sobre o impacto do tratamento de dados em vista da privacidade da sociedade como um todo, por isso a confiança pública deve ser mantida para que os cidadãos se sintam confortáveis. A autoridade só será eficaz se trabalhar em conjunto com reguladores, legisladores e outros autores. Esse entendimento resultou na criação do grupo *Digital Regulation Cooperation Forum* (DRCF), em que as áreas de concorrência, comunicação e proteção de dados começaram a trabalhar juntas. Assim, foi publicado um Plano de Trabalho conjunto[4] para que haja coerência na regulação de assuntos de

[4] Disponível em: < https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122 >. Acesso em 15 de junho de 2021.

interesse coletivo no Reino Unido.

Painel 1 - Regulação voltada para resultados: engajamento cooperativo, supervisão eficaz e execução inteligente

ARTHUR SABBAT, Diretor da ANPD, entende que a autoridade brasileira é jovem e, por isso, a primeira atividade foi fixar uma Agenda Regulatória específica com 10 ações para atuação da ANPD. Escolheu-se os temas pelo potencial impacto da regulamentação a ser construída para a sociedade e indivíduos de forma geral, além dos benefícios para a sociedade e respeito aos seus direitos.

Segundo **ANNA MORGAN,** representante da Autoridade de Proteção de Dados da Irlanda, a autoridade irlandesa também está no processo de definição de prioridades, e há dificuldade de definir quais questões deverão ser analisadas, já que os recursos são finitos. Equilibrar os interesses e riscos do tratamento de dados é um desafio ao lidar com as demandas da sociedade. Por isso, até maio de 2020, a autoridade analisou casos que foram reportados; mas, em regra, as reclamações foram de caráter individual relacionadas às áreas trabalhista e consumerista. Ou seja, não foram casos de impacto sistêmico ou coletivo. Ao mesmo tempo, muitas questões devem ser enfrentadas a nível mais amplo do que o indicado pelo RGPD, além de apoios a projetos de *compliance* realizados por empresas e de análise minuciosa sobre o volume das questões levadas à autoridade.

ZEE KIN YEONG, Comissário adjunto da Autoridade de Proteção de Dados de Singapura, entende que a lei de proteção de dados de Singapura assegura proteção aos dados pessoais dos consumidores e prevê que as empresas tenham uso legítimo dessas informações. São esses dois elementos que centram a atuação da autoridade. Para a Autoridade de Singapura, é fundamental disseminar boas práticas, e esta estratégia tem sido seguida no caso de compartilhamento de conhecimento com o Conselho de Singapura, voltado para o setor privado. Este Conselho cuida das empresas e estabelece diretrizes para a organização corporativa, a fim de que a proteção de dados seja respeitada desde os órgãos decisórios das empresas. Por isso, a autoridade busca reconhecer as empresas que adotam práticas relevantes para proteção de dados por meio de certificados, dessa forma as empresas passam a atuar com apoio da autoridade para que haja transparência, mas também proteção dos interesses das empresas. Esse sistema organizado pela autoridade de proteção de dados também auxilia a reputação das empresas sobre hábitos de privacidade, de forma a criar incentivos efetivos para que as grandes corporações adotem boas práticas.

Para **GUILHERME ROSCHKE**, Advogado para a Proteção Internacional do Consumidor na *Federal Trade Commission* dos Estados Unidos, uma das questões atuais é o viés discriminatório dos algoritmos, diante de testes e *inputs* falhos. Assim, o ponto de partida para solucionar essa questão é a transparência e a responsabilidade; os desenvolvedores devem garantir que decisões são defensáveis e explicáveis e deve ser possível que terceiros testem esses sistemas. Porém, a transparência não pode gerar ônus desproporcional aos consumidores, como na elaboração de políticas de privacidade demasiado longas. Ainda, no caso da tecnologia de reconhecimento facial, há estudos sobre a dificuldade desse instrumento funcionar de forma eficiente com indivíduos não brancos e isto apresenta um risco elevado. Outra pauta é proteger dados de jovens, já que o uso de tecnologias para educação foi ampliado de forma significativa em vista da pandemia.

Outra ferramenta utilizada para solucionar investigações relacionadas a violações de privacidade é a responsabilização, de forma a não se resumir nas consequências negativas financeiras, mas também de significar um incentivo às empresas em adotar técnicas de *compliance* pelas vantagens competitiva e reputacional. Logo as empresas vão perceber que práticas contra proteção de dados não são lucrativas e que é relevante ter medidas de *accountability* para fomentar formas de transparência para proteção das vítimas que sofreram danos, além de analisar questões de viés algoritmo. Ainda, isso é determinante para o estabelecimento de regras claras e transparentes para que as empresas saibam o que fazem e quais práticas são consideradas desleais.

Também é importante a realização de *Workshops* para conscientização dos consumidores e da sociedade civil, a fim de que todos conheçam e tenham experiências para saberem como agir em casos concretos. Essa prática auxilia na formação de um entendimento sobre a lei e na definição do que é permitido ou não, a fim de delimitar situações que devem ser levadas ao litígio judicial. Outra atividade é a cooperação, isso é feito por meio de normas que preveem a troca de informações e o compartilhamento de experiência e *know-how*. Todas essas medidas são eficazes quando concretizadas de forma conjunta para que os setores conheçam sobre os assuntos e promovam mudança de comportamentos.

Na visão de **CHRIS HODGES**, professor de Oxford, há uma tendência global para que as regulamentações sigam uma abordagem de risco, mas esse movimento deve ser seguido por ações centradas na mudança concreta de comportamento na relação entre empresas e indivíduo. Isso porque, em regra, a motivação para mudança está ligada no comportamento de indivíduos e não necessariamente nas respostas regulatórias e de punição previstas em uma lei. No caso de pequenas empresas, é interessante que se ofereça apoio para que haja maior engajamento delas

nos temas de proteção de dados, ao passo que o sancionamento poderá levar ao fechamento dessas empresas. Assim, as autoridades têm papel de se comunicar com as pessoas chave, como os diretores de empresas, a fim de influenciar de forma eficaz comportamentos, além de somar às abordagens de risco e de resultado para alocação de recursos. Ainda, regulações éticas e códigos de boas-prática são questões a serem seguidas em empresas para que haja promoção de cultura de proteção de dados.

EDUARDO BERTONI, Coordenador do *Instituto Interamericano de Derechos Humanos* e ex-Diretor da *Agência Argentina de Acesso à Informação Pública*, entende que uma das prioridades da autoridade argentina foi transformá-la em uma estrutura o mais independente possível. Até 2016, a Autoridade estava ligada ao Ministério da justiça e direitos humanos argentino e, por isso, os diretores integrantes da autoridade poderiam ser removidos a depender da discricionariedade do Ministro da Justiça. Desde então, percebeu-se a necessidade de haver maior independência da Autoridade, e, por isso, essas questões passaram a ser de escopo da Agência de Acesso à Informação. Logo, nota-se que houve esforço conjunto para que fosse observada essa estrutura independente e autônoma. Além disso, a participação da Autoridade em fóruns internacionais reforça a independência e beneficia o órgão na aplicação da lei, como é o caso da Convenção 108 para cooperação na investigação. No caso do Brasil, a LGPD deve ser implementada para garantir maior autonomia à Autoridade de proteção de dados (ANPD). Ainda ressaltou que esse tema deve ganhar maior relevância no debate do Mercosul, que há de ser reforçado no futuro.

Painel 2 - O papel da prestação de contas na proteção de dados: criando programas de governança de dados baseados na avaliação de riscos e demonstração de conformidade

O objetivo deste painel foi compreender como as empresas implementaram práticas específicas no contexto da prestação de contas e proteção de dados. Há uma expectativa crescente por parte das leis e regulamentos de que as organizações devem ser responsáveis e ter políticas de privacidade e boas práticas fortes relacionadas. Essa realidade é acompanhada pela tendência de estabelecer a agenda de negócios das empresas e o interesse dos conselhos empresariais focados na privacidade para além da conformidade legal. Além disso, a pandemia da COVID-19 transformou a *accountability* como bússola institucional para o mundo pós-COVID.

Nessa perspectiva, **ROB SHERMAN**, vice-presidente de privacidade do Facebook, destacou a necessidade de se pensar nas práticas internacionais de prestação de contas e

fiscalização, já que hoje muitas empresas atendem consumidores em todo o mundo e precisam se adequar à legislação de cada região. Por isso, construir uma abordagem de implementação regulatória que divida a implementação da lei em diferentes enfoques é um movimento relevante. Além disso, a possibilidade de consultar a autoridade de proteção de dados sobre suas expectativas quanto ao programa de conformidade é essencial para a tomada de decisões fundamentadas; em alguns casos, essa consulta externa pode ter a contribuição da academia e da sociedade civil organizada. O investimento na área de segurança e o desenvolvimento de avaliações de risco têm um papel importante para tornar a empresa responsável, pois ajudam a manter a consistência e a auditabilidade ao longo do tempo.

Em complementação, **CAROLINE LOUVEAUX**, Diretora de Privacidade da Mastercard, concordou que uma cultura de proteção de dados começa no nível mais alto da organização. No contexto da prestação de contas, a empresa implementou instrumentos de privacidade e segurança na Europa e obteve as certificações CBPR (*Cross Border Privacy Rules Certification*), pois são ferramentas que demonstram que o negócio está em conformidade com os requisitos das leis de privacidade. Para ilustrar atividades relacionadas à adequação, **CAROLINE** apontou a implementação de ferramentas e mecanismos de governança para garantir o cumprimento efetivo das normas, a rede de escritórios de privacidade e proteção de dados, e a realização de auditorias nas práticas de dados. Via de regra, **CAROLINE** acredita que é mais eficaz ter um único programa de conformidade com base nos padrões mais elevados de privacidade e ajustar a partir disso, em vez de ter vários programas diferentes descentralizados. A executiva afirmou a utilidade de ter uma política específica para casos de incidente de segurança a fim de que os colaboradores da empresa possam entender o que fazer e como agir rapidamente. Por fim, ela falou sobre o setor de conscientização e treinamento especializado na realização de *tabletop exercise* todos os anos.

RENATO MONTEIRO, Líder do Conselho de Proteção de Dados do Twitter na América Latina, descreveu um movimento de compreensão da privacidade como um objetivo corporativo. Como consequência, a privacidade e a segurança da informação passaram a compor os parâmetros de progressão de carreira da empresa e qualquer colaborador que tiver interesse pode obter a certificação de privacidade. Outra prática da empresa é manter o diálogo aberto com reguladores sobre o processo de revisão de práticas de privacidade; isso ocorreu com a ICO, por exemplo. Além disso, o Twitter indica em seu site a base legal para o tratamento de dados pessoais e mantém publicamente os resumos da avaliação de interesse legítimo. A nível mundial, a empresa mantém um programa de privacidade global, porém tem sido cada vez mais frequente o estabelecimento de abordagens regionais baseadas em riscos e benefícios.

Segundo **ROBERTO BRUCE**, Gerente de privacidade de dados do Bradesco, o aspecto da *accountability* permeia toda a regulação de proteção de dados e, nesse sentido, a LGPD fomenta a adoção de boas práticas pelos agentes de tratamento. Para entender e aplicar o princípio da *accountability*, a empresa decidiu atuar de forma dedicada junto a Federação Brasileira de Bancos (FEBRABAN) para adotar caminhos recomendados, implementar um guia de boas práticas e produzir vídeos e cursos informativos. Ainda, a diretoria nomeou o encarregado de dados (DPOS) e indicou o nome e contato dele no site do banco, além de criar meios para concretização dos direitos pelos titulares de dados.

MARLON DOMINGUES, encarregado (DPO) da *Erasmus University* de Rotterdam, notou que, no caso de empresas locais, para responsabilização, é necessário estabelecer uma liderança para conduzir o programa de conformidade e desenvolver políticas de privacidade, além de outros padrões atualizados e específicos. Outro aspecto relevante é construir uma estrutura para o programa de privacidade, pois, no caso de organizações do setor de educação, a empresa pode ser observada em três níveis: dentro da organização, nas colaborações internacionais e no setor de ensino superior.

Por outro lado, apesar do Banco Mundial ser uma organização internacional, que está isenta de seguir qualquer regulamentação específica de países, como o RGPD ou a LGPD, a instituição percebe os riscos de ignorar questões em relação a utilização de dados pessoais, especificamente nas pesquisas realizadas pelo banco. Para **TAMI DOKKEN**, do Gabinete de Privacidade de Dados do Banco Mundial, os riscos incluem prejuízos a negócios jurídicos e à própria reputação do banco. Devido a isso, o Banco implementou voluntariamente a primeira política de privacidade de dados pessoais que entrou em operação em fevereiro de 2021. Especificamente sobre responsabilização, a política de privacidade do Banco prevê formas de responsabilidade interna e externa, e a governança de privacidade de dados é utilizada com o modelo padrão de três linhas de defesa em que todos os funcionários são responsáveis por integrar a privacidade dos dados ao seu trabalho diário. Além disso, o Banco realizou uma avaliação de risco de cada região de unidade de negócios e grupo de prática para identificar as atividades da organização que envolvem dados pessoais e assim cobrir quaisquer lacunas que tenham sido identificadas.

MARCOS OTTONI, coordenador jurídico da CNSaúde, destaca que o setor de saúde está sendo chamado não apenas a adequar suas políticas internas e implementar diretrizes de privacidade, mas também a usar racionalmente os dados pessoais para o combate à pandemia. Portanto, a organização observou a possibilidade de prever boas práticas mínimas de privacidade a nível individual, mas também em associações. Diante disso, a CNSaúde lançou o

Código de Boas Práticas para Prestadores Privados em Saúde[5]. O estabelecimento desta política entre as organizações que compõem o CNSaúde serve tanto para proteger os titulares como para garantir simetrias comerciais e evitar distorções competitivas. Na opinião da entidade, o Código será aprimorado de acordo com a utilização do documento, não é um texto fixo que não observa questões concretas. Para isso, é importante atuar ao lado das autoridades públicas, tanto de proteção de dados, como do setor da saúde, para que as questões sejam debatidas de forma fundamentada.

Abertura do Segundo Dia

De início, **GIOVANNA CARLONI** e **LAURA SCHERTEL** pontuam que a discussão do dia tratará sobre transferência internacional de dados e incidentes de segurança. Destaca-se que essa discussão está ligada intimamente com os temas do dia anterior (modelos regulatórios e *accontability*), já que os procedimentos oriundos desses tópicos são essenciais tanto para a transferência internacional de dados quanto para a dinâmica do gerenciamento de incidentes de segurança.

Keynote – Encarregados (*data protection office – DPO*) e a ascensão das profissões de privacidade

O primeiro palestrante foi **TREVOR HUGHES,** CEO e Presidente da *International Association of Privacy Professionals - IAPP*, maior comunidade do mundo de profissionais que trabalham com o tratamento de dados. Trevor levanta a questão de que a profissionalização dos envolvidos no tratamento de dados é ponto central para uma efetiva proteção de dados, e que o Regulamento Geral de Proteção de Dados (RGPD, norma geral europeia sobre o tema) exaltou essa necessidade. No Brasil, por exemplo, estima-se que serão necessários 50 mil profissionais na área. Nesse contexto, coloca-se como essencial um profissional bem treinado, o que agrega grande valor à proteção de dados e à economia digital. Assim, expõe que a principal função da IAPP é exatamente criar mecanismos, como treinamentos e a incremento de cursos superiores na área, com fins de capacitar os encarregados da proteção de dados.

Keynote – Uma nova forma de proteção de dados: o Reino Unido está abrindo um novo

[5] Disponível em: < http://cnsaude.org.br/baixe-aqui-o-codigo-de-boas-praticas-protecao-de-dados-para-prestadores-privados-de-saude/ >. Acesso em 15 de junho de 2021.

caminho?

Após Trevor, foi a vez de **JAMES SNOOK,** Diretor da Política de Dados no *Department for Digital, Culture, Media and Sport (DCMS)* do Reino Unido, onde exerce como principal função a formulação de regulamentos sobre proteção de dados. Na apresentação, tratou principalmente da Estratégia Nacional de Dados do Reino Unido, publicada em 2020[6]. A importância do documento foi justificada em três eixos: (i) o valor econômico dos dados na modernidade; (ii) o valor de tais ativos às instituições públicas para aprimorar sua eficiência; e (iii) os riscos oriundos do tratamento de dados para os direitos individuais.

Assim, de todo exposto, entende-se que o principal objetivo da Estratégia consiste em minimizar os riscos e potencializar as oportunidades provenientes das novas tecnologias e do tratamento de dados. Para tanto, separou o intuito da Estratégia Nacional em cinco missões:

(i) garantir um ambiente onde se consiga explorar com afinco o valor econômico dos dados;

(ii) criar um ambiente pró-crescimento, que considere as limitações de cada organização para assim definir seus encargos em matéria de proteção de dados;

(iii) maximização da eficiência pública na prestação de seus serviços através do tratamento de dados;

(iv) estabelecimento de uma forte estrutura de gestão de risco, em face da crescente dependência que temos da tecnologia e do tratamento de dados; e

(v) criar uma forte estrutura legal e regulatória para o estabelecimento de um ambiente seguro para a transferência internacional de dados, colocando o Reino Unido como líder internacional para o desenvolvimento deste pilar.

Painel 3 – Viabilizando transferências internacionais de dados

A primeira painelista foi **MIRIAM WIMMER,** diretora da Autoridade Nacional de Proteção de Dados – ANPD. **MIRIAM** falou sobre o fato de a proteção de dados ser tema incipiente no Brasil, o que faz com que as discussões andem em um ritmo mais lento. Mesmo assim, afirmou que a ANPD está colocando prioridades para o desenvolvimento do tema no Brasil, entre eles, o fluxo transfronteiriço de dados, que tem espaço regulatório previsto para o

[6] Disponível em: < https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy >. Acesso em 15 de junho de 2021.

primeiro semestre de 2022, conforme a agenda regulatória publicada pela Autoridade. Nesse contexto, **MIRIAM** encerrou sua apresentação afirmando que o foco inicial será uma regulamentação focada na prática de transferência de dados no dia a dia das empresas, questão mais simples e urgente.

O próximo expositor foi **YUJI ASAI,** da Autoridade responsável pela proteção de dados no Japão. O palestrante tratou sobre o reconhecimento mútuo entre o Japão e a União Europeia para o livre fluxo de dados, afirmando que essa adequação se dá por meio da confiança, que, por sua vez, é construída a partir de estruturas de proteção de dados parecidas, independente de diferenças culturais entre os países ou regiões. Apresentou, por último, sobre a existência de certificados de livre fluxo de dados, que atesta a confiança entre os países e que pode servir para o Brasil no futuro.

O terceiro foi **JOE JONES,** também do *Department for Digital, Culture, Media and Sport (DCMS)* do Reino Unido. O palestrante também falou sobre a necessidade de uma cultura de proteção de dados, que varia de país para país a depender de sua história. Nesse sentido, ressaltou que, para o estabelecimento de adequação mútuas para a livre transferência de dados, prescinde-se de correspondência nas normas em si, mas é necessária uma identidade na estrutura de proteção de dados e nos princípios gerais que a guiam. Além disso, deu destaque ao fato de que o processo de adequação deve ocorrer com senso de mutualidade e espírito cooperativo, e não com um país ou região dispondo regras que o outro deve aceitar. O acordo com o Japão é um exemplo nesse sentido, vez que guiado com muito diálogo.

Em seguida, foi a vez de **KATE CHARLET,** do Google. A palestrante começou falando da importância da computação global. Segundo ela, a rede interligada em todo globo ajuda, inclusive, na segurança da informação, auxiliando, por exemplo, no mapeamento do tráfego em um sistema. O que pretende demonstrar com isso é que um fluxo livre global não significa necessária ameaça à privacidade. Ademais, a executiva da Google buscou ressaltar a importância do fluxo livre de dados para toda a sociedade, perfazendo o caminho desde as facilidades que todas as empresas encontram quando não há barreiras para esse fluxo até os benefícios que isso faz repercutir na vida do consumidor. Por fim, destaca que tal liberdade não é paradoxal com a proteção de dados, e que ambas devem se ajustar e subsistir.

O quinto palestrante foi **JACOBO ESQUENAZI,** da HP. A grande questão debatida pelo executivo diz respeito aos certificados de confiança para as empresas emitidos por alguns países. **JACOBO** afirmou que esse é um ótimo instrumento para adequação as normas mais rígidas de proteção e transferência de dados, visto que, para uma adequação em ordem global, a empresa terá que lançar mão de um código de conduta que se adeque às regras dispostas nas

regiões que atua. Destaca que uma das principais dificuldades para os países construírem seus certificados é a falta de uma massa crítica para julgar os casos. Tendo isso em vista, por fim, recomenda que o Brasil aprove ou reconheça os certificados já existentes.

O último a falar no painel foi **MARCEL LEONARDI,** sócio do escritório Leonardi Advogados. Este apresentou a problemática oriunda da ausência de mecanismos de transferências internacionais de dados no contexto normativo brasileiro, tendo em vista a necessidade incessante de as empresas realizarem operações de tratamento de dados transfronteiriças. Entre seguir a legislação europeia para transferência de dados e outras possibilidades, **MARCEL** consignou que a melhor alternativa é que as empresas estabeleçam um debate intenso com a ANPD para que essa forneça as diretrizes para o fluxo internacional de dados enquanto não há regulamentações sólidas nem outros instrumentos sobre o tema.

Painel 4 – Notificação e gerenciamento de incidentes de segurança: um desafio para as organizações e para as Autoridades de Proteção de Dados (DPAs)

O primeiro palestrante foi **JOACIL BASÍLIO RAEL,** Diretor da ANPD. O palestrante exaltou a gravidade que os incidentes podem ter, principalmente quando envolvem dados sensíveis, gerando danos individuais e coletivos irreversíveis. Afirmou que, tendo tal contexto em vista, a ANPD adotou como prioridade a regulamentação sobre incidentes de segurança, sendo que, já em 2021, foi aberta uma Tomada de Subsídios pela Autoridade, a fim de orientar detalhadamente a sociedade civil, o que irá culminar em tais normativas complementares.

O próximo a expor no painel foi **DAVID STEVENS,** da Autoridade de proteção de dados belga. A partir da experiência da Bélgica após a entrada em vigor do RGPD, David afirmou que é comum um crescimento de notificações de violações de dados a partir da vigência de norma sobre o tema. Nesse contexto, alegou sobre a importância de determinadas medidas, como (i) ter bons critérios organizacionais, por exemplo mediante a implementação de softwares que separam e organizam as notificações que chegam, (ii) conseguir separar e dar maior atenção para o que realmente for importante e apresenta potencial de aprendizado e (iii) comunicar à sociedade sobre os incidentes com cautela, levando somente as informações certas sobre o caso, sem muito alarde.

Em seguida, falou **BRIDGET TREACY,** sócia do Hunton Andrews Kurth. A palestrante ressaltou que os incidentes fazem parte do dia a dia das empresas; eles não vão desaparecer, as companhias que devem aprender a lidar com eles. Para tanto, destacou que, em primeiro lugar, as empresas devem aprender a identificar o incidente, tarefa muitas vezes árdua; em seguida,

destacou a importância de mecanismos internos de comunicação de incidentes, isto é, incentivar o uso de relatórios dentro da própria empresa que comuniquem o ocorrido; por fim, consignou sobre a dificuldade e o curto espaço de tempo para notificar os afetados pelo incidente, considerando a complexidade de muitos casos. Sobre esse último ponto, destacou a importância de as Autoridades entenderem que o primeiro contato sobre o incidente será mais raso, enquanto a empresa trata e entende melhor o problema que ocorreu.

Posteriormente, foi a vez de **FLAVIA MITRI,** da Uber. Em sua exposição, a executiva falou um pouco da experiência da empresa, que já enfrentou muitas dificuldades na tarefa de relatar incidentes de segurança. Afirmou que, com o passar do tempo, construiu um time sólido e preparado para lidar com a questão dos incidentes, sendo que as equipes trabalham espalhadas por todo o mundo, cumprindo as regras específicas do local onde se constatou o problema. Outro ponto de destaque diz respeito a diferença de comunicação sobre incidentes de segurança para os titulares e para as autoridades de controle. Para estas, Flavia consignou que a comunicação é técnica e só ocorre quando é legalmente necessário; já para os titulares dos dados devassados, afirmou que a empresa preza por uma comunicação mais humanizada e cuidadosa, ocorrendo independente de imposição legal.

A quarta especialista a falar foi **MARIE OLSON,** da Boeing. Marie ressaltou a importância de se adotar um plano de ação antes mesmo de ocorrer os incidentes, assim a empresa terá toda a estrutura pronta para executar cada um dos esforços necessários diante do problema. Por exemplo, um grupo estará tentando corrigir o incidente, enquanto outro, investigando as causas e outro, comunicando às pessoas necessárias. Além disso, deu-se destaque para pequenos detalhes que são importantes para evitar os incidentes; como exemplo, foi citado a criptografia dos discos de laptops, e até mesmo dicas para os funcionários não serem roubados, como não deixar suas máquinas no banco da frente do carro ou não as levar em viagens em que são desnecessárias.

O quinto painelista foi **NICOLAS ANDRADE,** do Zoom. Tratou-se sobre a necessidade de se investir em uma forte equipe de privacidade que desenvolva seu trabalho de forma integrada com o resto da empresa, atitude adotada pelo Zoom, principalmente pelo grande aumento de demanda durante a pandemia. Ademais, o executivo ressaltou outros aspectos importantes, como aumentar o tempo para a comunicação dos incidentes de segurança aos titulares dos dados violados e a simplificação dos formulários de aviso de incidente, retirando, por exemplo, a necessidade de CPF/CNPJ do controlador de dados, já que há empresas que não estão localizadas fisicamente no território brasileiro.

Por fim, falou **CRISTINE HOEPERS,** do CERT.br. Cristine buscou deixar claro a

importância da gestão de incidente, área dentro de uma empresa que deve circular pela proteção de dados, segurança da informação e outros setores. Para a painelista, é de extrema importância saber o que fazer antes e depois que ocorrem os incidentes, e é esse o principal papel do grupo de gestão de incidente. Nesse sentido, destaca que se deve incentivar os encarregados (DPOs) a adquirirem conhecimento além do jurídico, desenvolvendo habilidades técnicas úteis para a prevenção e contenção de incidentes.