Relatoria - 12º Fórum da Internet no Brasil - Natal/RN

DataPrivacyBR Research

Título do workshop

Dados Virais: Legado da COVID-19 nas aquisições de tecnologia pelo poder público no Brasil

Tema do workshop

No Brasil, diferentes esferas de governo desenvolveram e adquiriram tecnologias para mitigar riscos e danos relacionados à COVID-19. Aplicativos, inteligência artificial, câmeras com diversas funcionalidades e bancos de dados foram utilizados em todo o território nacional para monitorar a evolução da pandemia e evitar novos contágios. Por outro lado, há pouca transparência sobre como essas soluções tecnológicas funcionam e quais são seus possíveis impactos em relação à privacidade e à segurança dos cidadãos. A partir dos questionamentos e resultados encontrados no projeto dados virais, uma investigação que identificou 253 tecnologias baseadas em dados pessoais, usadas no combate à Covid-19, no Brasil em 2020. O painel tem como objetivo reunir especialistas de diferentes expertises para debater políticas de saúde pública baseada em dados, destacando seus riscos e potencialidades. Além disso, busca apontar medidas a serem tomadas pelo poder público para garantir segurança e transparência em outros projetos similares, relacionando Lei de Acesso à Informação e LGPD.

Proponente:
Associação Data Privacy Brasil de Pesquisa (Terceiro setor)

Moderação:
Pedro Saliba (terceiro setor)

Relatoria:
Gabriela Vergili (terceiro setor)

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

Estruturação do workshop

O painel é fruto de uma pesquisa realizada pela Associação Data Privacy Brasil chamada Dados Virais, que teve como objetivo mapear a adoção de tecnologias baseadas no tratamento de dados pessoais para combate à COVID-19 durante o período de calamidade pública pelo poder público brasileiro. Como resultado, nós tivemos um panorama geral da utilização dessas tecnologias, as localidades e áreas de abrangência, atores envolvidos em tais arranjos e principais funcionalidades e por essas tecnologias adotadas e se puder. Todos os resultados foram apresentados em em uma plataforma online, e pormenorizados em um relatório sobre a etapa de mapeamento e um relatório de estudos de caso.

Objetivos e resultados (pretendidos e obtidos)

O presente workshop teve como objetivo apresentar um panorama de políticas de saúde pública baseadas em dados, apontando seus riscos e potencialidades. O painel privilegiou arranjos entre setor público e privado para entender o desenvolvimento e aplicação de diferentes tecnologias em um contexto de emergência sanitária, abordando questões sobre boas práticas e transparência, responsabilidades advindas tanto da Lei Geral de Proteção de Dados e da Lei de Acesso à Informação. Quais foram as tecnologias mais implementadas no país? Quais foram os arranjos contratuais estabelecidos entre poder público e setor privado? Existem grupos sociais mais vulneráveis à produção de dados pessoais nessas políticas públicas? Houve preocupação com fundamentos da proteção de dados pelas instituições responsáveis? Qual a importância da transparência por agentes públicos e privados sobre os usos das tecnologias? Como a experiência da pandemia pode auxiliar em futuras políticas públicas que realizem a coleta e tratamento de dados para sua execução?

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

Justificativa em relação à governança da internet

O workshop trouxe a perspectiva de diferentes atores sobre as estratégias institucionais para utilização de tecnologias em um contexto de isolamento social. Um dos primeiros questionamentos abordado no painel foi em que medida o uso de tecnologias para o combate à COVID-19 interfere em questões de privacidade e proteção de dados. Portanto, a relevância entre o painel e o primeiro princípio do Decálogo (liberdade, privacidade e direitos humanos) é marcada e guarda relação com a principal pergunta orientadora que conduzirá o debate.

Além disso, ao passo em que a digitalização dos serviços públicos e isolamento social ocorreu em um contexto de urgência na adoção de tecnologias para tomadas de decisões, nota-se o condão de inovação que permeia as políticas públicas adotadas. Nesse sentido, esse processo foi marcado por uma articulação com o setor privado que não apenas permitisse oferecer respostas e soluções em tempo hábil para a leitura e o combate à pandemia, como também que estivesse atento à preservação de liberdades e direitos fundamentais. Desta forma, além da relação com o princípio de direitos humanos, são também marcantes no painel o princípio da inovação e o princípio da governança democrática e colaborativa, reiterando a importância da discussão para a Governança da Internet. Mais ainda, o painel também explorou o ambiente legal e regulatório de novas tecnologias, preservando a dinâmica da internet como um espaço de colaboração.

Metodologia e formas de participação

O painel utilizou o formato de mesa redonda, com perguntas orientadoras de estímulo do diálogo. Houve uma breve apresentação do tema com exposição de alguns resultados do projeto Dados Virais, oferecendo ao público um panorama geral da adoção de tecnologias para combate à COVID-19 pelo poder

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

público em 2020. Em seguida, algumas perguntas orientadoras foram feitas a cada painelista, com tempo de exposição de 10 minutos cada, para compreender de que forma pensam as relações entre dados pessoais e políticas públicas de acordo com sua expertise e atuação na pandemia. Em seguida, propõe-se aos convidados responder a dúvidas do público (que acompanharam o painel presencial ou remotamente) que, embasados com os resultados da pesquisa apresentados anteriormente e suas próprias experiências, poderão trazer novas questões para o debate multisetorial.

Foram mobilizadas as redes sociais da proponente para realizar divulgação prévia do evento, expondo os pontos de debate e link para acesso virtual (Twitter e Instagram, além do chat do vídeo de transmissão ao vivo para a audiência remota). Durante o evento, realizamos uma thread no Twitter relatando em tempo real, de forma resumida, as falas proferidas e as principais questões levantadas.

Mesa Redonda

Dayana Costa - Empresarial

Gerente de Privacy da Incognia Tecnologia da Informação, com especialização em Privacidade e Proteção de Dados pelo Data Privacy Brasil, MBA em Direito Digital pela Escola Paulista de Direito, especialização em Direito Digital pela FGV, coordenadora adjunta da Comissão de Direito Digital da OAB Subseção de Santo Amaro, indicada pela Revista Análise Edição Mulheres como uma das advogadas mais admiradas do Brasil na área de Direito Digital no ano de 2021, professora convidada em cursos e palestras sobre proteção de dados e autora de diversos artigos jurídicos sobre o tema privacidade e proteção de dados.

Segundo Dayana, o cenário pandêmico trouxe desafios para o setor público, privado e sociedade em geral, criando estratégias centradas em dados para combater à COVID-19. O foco é em um elemento central: a informação. Nesse contexto, a In Loco (atualmente denominada Incognia) criou o Índice de Isolamento Social, uma adaptação de uma ferramenta que anteriormente à

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

pandemia era uma tecnologia de geolocalização utilizada para fins mídia e publicidade. Para garantir a segurança neste processo, foi formado um grupo de trabalho interno para definir a forma de condução do fornecimento da ferramenta e adequação às normas de proteção da privacidade dos usuários. Algo que facilitou o processo, foi o fato de que a empresa foi construída a partir do princípio de *privacy by design*, assim, desde sempre já aplicava medidas como *hash* e criptografia na segurança do Índice de Isolamento Social, ofertando uma métrica estatística baseada em geolocalização.

O funcionamento do Índice de Isolamento Social dependia de dois elementos: 1) assertividade da ferramenta e segurança sobre os dados que seriam utilizados para políticas públicas; e 2) volume de dados, com mais de 60 milhões de dispositivos no Brasil, permitindo uma análise estatística de muitos locais. O Índice separava o território em polígonos de 450 metros de raio, identificando os dispositivos que estavam à noite nesse polígono e se pelo dia haveria deslocamento dessa área. Se acontecesse, o produto apontava que não havia isolamento.

Havia também uma preocupação da In Loco (Incognia) foi com a privacidade, no sentido de não compartilhar esses dados com o governo de maneira que eles pudessem identificar qualquer titular. Os dados eram disponibilizados de forma agregada com períodos de 24 a 48 horas após a coleta, de modo a não haver uma vigilância do governo sobre essas pessoas. Os contratos celebrados seguiam as disposições da LGPD, ainda que ela ainda não estivesse em vigor, adicionando cláusulas robustas para utilização apenas para finalidade específica. A finalidade era bem delimitada e não continha dados de identificação como nome, RG, CPF ou e-mail. Havia uma segregação lógica e os dados não eram cruzados com outras informações.

Além disso, prezou-se pela transparência. Foi publicada uma política de privacidade detalhada, explicando quais os tipos de dados que estavam sendo coletados e suas finalidades, além de um site com principais dúvidas. Foi exigido dos parceiros da In Loco (Incognia) que publicassem suas políticas e seus termos de

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

uso a informação do uso desses dados. Foi aberto um diálogo com a sociedade, com participação em fóruns e de eventos de discussão.

Dayana conclui afirmando que é possível utilizar tecnologias para combater a COVID-19, desde que sejam respeitadas as regras de privacidade, de proteção de dados e ressalta que essas ferramentas não podem ser utilizadas como uma vigilância para uma intrusão na vida privada das pessoas.

Paulo Victor Purificação Melo - Comunidade científica

Doutor em Comunicação e Cultura Contemporâneas pela Universidade Federal da Bahia, realizando pós-doutorado na Universidade da Beira Interior, em Portugal, como pesquisador do LabCom – Comunicação e Artes. Coordenador do Centro de Comunicação, Democracia e Cidadania da UFBA. Atualmente é também bolsista de pesquisa da Fundação Oswaldo Cruz - Fiocruz, no projeto "Proteção de Dados em Serviços de Saúde Digital". Coordenador do GP Comunicação Antirracista e Pensamento Afrodiaspórico da Intercom - Sociedade Brasileira de Estudos Interdisciplinares da Comunicação e integrante do Conselho Consultivo da mesma entidade. Coordenador do Grupo de Trabalho Políticas e Governança da Comunicação da Compolítica - Associação Brasileira de Pesquisadores em Comunicação e Política.

Apresenta uma perspectiva crítica do sobre a decisão apressada da adoção de tecnologias ou, em outras palavras, o tecnosolucionismo, a crença de que estas ferramentas são suficientes para a resolução de problemas extremamente complexos e que envolvem questões políticas, econômicas, sociais, culturais, raciais e territoriais. Esses pontos são anteriores à COVID-19, mas se agravaram de forma bastante considerável a partir da pandemia.

No início da pandemia, estava colocado o desafio de executar uma atuação rápida sem colocar em risco a população no que diz respeito ao seu direito à privacidade e à proteção dos seus dados pessoais. Aborda o aspecto do quanto essa discussão assume um

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

caráter público ou em que medida essa adoção das tecnologias se deu a partir de diálogos entre poder público e iniciativa privada, como no caso de compartilhamento dos dados de empresas de telefonia com o IBGE.

Afirma que há uma disposição do Estado brasileiro para colocar em risco esses direitos digitais, exemplificando com a falta de medidas de transparência em relação ao funcionamento das tecnologias, plataformas digitais e seus acordos celebrados.

Não há no Brasil instituições públicas sólidas, que supervisionem efetivamente esse cenário, sendo visível também um forte interesse comercial para acesso aos dados coletados. Um país no qual o interesse comercial exerce influência sobre as decisões políticas dos diferentes níveis e também um país em que as tecnologias digitais têm sido utilizadas para vigilância, para a segregação e para o controle dos corpos, particularmente aí pessoas negras de mulheres e transsexuais.

Em pesquisa que participa na Fiocruz, fala que a adoção dessas tecnologias, sobretudo por secretarias de saúde, não têm passado por uma discussão entre os próprios trabalhadores e trabalhadoras de serviço de saúde antes de sua implementação. Trouxe ainda o ponto sobre tratamento de dados pessoais em políticas de assistência social, como INSS, Cadastro Único e outros.

Do ponto de vista da população, temos ainda uma série de desafios. O primeiro é o nível de cultura de proteção de dados no Brasil, que ainda é baixo. Quando as pessoas estão com fome ou num severo estado de insegurança alimentar, quando estão desempregadas, sem perspectiva de conseguir emprego ou quando estão perdendo suas casas, qual o lugar que a questão dos dados pessoais aparece na vida dessas pessoas? Por exemplo, para um jovem negro das periferias brasileiras, a importância de ter o RG consigo é tentar manter-se vivo no momento de uma abordagem policial ou o CPF que uma dona de casa hipertensa utiliza para conseguir descontos em remédios na farmácia. Há direitos básicos em jogo neste contexto.

DataPrivacyBR Research

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

Paulo Melo pauta o desafio de ampliar o diálogo com o conjunto da população sobre qual é de fato a importância de proteger esses dados, de garantir a sua privacidade. Entende existir uma banalização do dado pessoal neste sentido. Propõe a ampliação dos canais de comunicação com a população, que passa, por exemplo, por incluir na sistemática das escolas públicas e privadas, na agenda política, nos sindicatos, associações de pais e movimentos populares.

Alessandra Gomes - Terceiro setor

Tech Fellow do InternetLab. Mestra em Ciência da Computação pelo Instituto de Computação da Universidade Estadual de Campinas (IC – Unicamp) e Bacharela em Ciência da Computação pela Universidade Federal do Pará (ICEN – UFPA). Atuou com desenvolvimento de Software no PROUCA (Programa Um Computador por Aluno), na startup NAPP Solutions e no Projeto Contare, da Rede Ovelha Negra, vencedor do Prêmio Simineral de Comunicação 2018, e como pesquisadora e professora no Instituto Federal de Brasília (IFB), no Programa PARFOR pela Universidade Federal Rural da Amazônia (UFRA) e no Projeto ProgrAmazonas, único aprovado em 2018 no Edital Elas nas Exatas na Região Norte.

Alessandra Gomes participou de um projeto de pesquisa sobre aplicativos de COVID-19 iniciado em meados de abril de 2020, trabalhando questões relacionadas à segurança e privacidade. Foram analisados oito aplicativos e a maioria deles tinha um objetivo informativo, orientando as pessoas sobre contágio, sintomas e formas de prevenção.

Para informar esse conjunto de informações os aplicativos geralmente vinham acompanhados de formulários solicitando dados. Durante a pesquisa, perguntou-se: se eram aplicativos informativos, por que solicitavam dados pessoais, nome completo das pessoas, e-mail, CPF, RG ou telefone? Muitos tinham esta coleta como pré-requisito para a utilização do aplicativo, vedando seu uso caso não fosse realizada.

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

Identificaram a ausência de termos de uso ou de política de privacidade em muitos deles.

A pesquisa analisou ainda as solicitações de acesso nos aplicativos para Android. Com frequência, foi observado que muitos pediam informação de geolocalização, sendo que dentro daquele aplicativo não tinha nenhuma funcionalidade que justificasse seu tratamento, como um mapa para indicar postos de saúde mais próximos à pessoa. Outros solicitavam acesso a câmera e áudio sem haver uma funcionalidade de telemedicina, por exemplo. Se o aplicativo não oferece essa funcionalidade, por que é realizada a coleta?

Analisaram, ainda, as atualizações que os aplicativos vinham tendo ao longo do tempo. Observaram a mudança de característica de alguns aplicativos: muitos que eram informativos com o passar do tempo, mudaram, se tornaram aplicativos de rastreabilidade.

Finaliza reiterando a banalização dos dados. Uma pessoa que vai utilizar o aplicativo não vai ter essa preocupação: ela vai preencher e permitir tudo, sem questionar-se sobre o tratamento dos dados.Sem transparência, não é possível saber como esses dados estão sendo utilizados, devendo direcionar as críticas para as pessoas, instituições e empresas responsáveis a partir de uma visão crítica.

Marcos Lindenmayer - Governamental

Auditor Federal de Finanças e Controle da Controladoria-Geral da União. Bacharel em Direito pela Universidade Federal do Rio Grande do Sul, foi Conselheiro da Comissão da Anistia no Ministério da Justiça. Chefe de Gabinete da Ouvidoria-Geral da União desde 2016, é responsável pelas ações de inovação, articulação social, federativa e internacional, normatização, criação de competências e capacitação de unidades de ouvidoria do Sistema de Ouvidoria do Poder Executivo Federal e coordena projetos como o de implementação dos Conselhos de Usuários de Serviços Públicos no Poder Executivo Federal e de ampliação do direito de acesso à informação a grupos em situação de

DataPrivacyBR Research

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

DataPrivacyBR Research

vulnerabilidade na América Latina. Desde 2019, é Secretário da Rede Nacional de Ouvidorias, que congrega cerca de 2,4 mil unidades em todos os entes e Poderes da União. Atuou na implantação da Lei de Acesso à Informação (Lei nº 12.527, de 2011), da Lei de Proteção e Defesa dos Usuários de Serviços Públicos (Lei nº 13.460, de 2017), da Lei de Defesa dos Informantes (Lei nº 13.608, de 2018) e, mais recentemente, da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 2018), sendo titular da CGU no Subcomitê de Implantação da LGPD do Comitê Central de Governança de Dados do Poder Executivo federal, um dos autores do "Guia de boas práticas para a implantação da LGPD no Poder Executivo federal" e representante do Brasil na Rede Iberoamericana de Proteção de Dados até 2020.

A pandemia impactou o processamento de pedidos de acesso à informação, especificamente na parte de transparência passiva. Mas também é possível expor algumas questões relacionadas à transparência ativa e política de dados abertos. Nesse primeiro ponto, aponta ser importante salientar que existem cenários bastante distintos, especialmente levando em conta a Lei de Acesso à Informação em estados e municípios.

No âmbito federal, do direito procedimental de acesso à informação, não houve um impacto relativamente grande porque a estratégia de implementação da Lei de Acesso à Informação no âmbito do Poder Executivo Federal acabou sendo uma estratégia digital, desde 2012. Os canais preponderantemente digitais que já estavam colocados continuaram a ser utilizados e seguiram dali para frente com um incremento substancial em termos de demanda. Além disso, é interessante apontar que houve um movimento curioso: os canais existentes já tinham bastante visibilidade em termos de acesso à informação e à sociedade, demandando cada vez mais a prestação de serviços ou tendo dificuldades em acessar serviços anteriormente acessíveis em meio meio físico e começar a utilizar das plataformas de acesso à informação para fazer as suas solicitações de serviços. Observa-se um processo positivo nesse aspecto: a popularização das solicitações de informações, algo antes não visto, exceto por movimentos de organizações civis.

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

A preocupação maior está no efeito da pandemia e, especificamente, na adoção de regimes de teletrabalho por grande parte da administração, sem haver uma preparação prévia para tanto. Se já havia uma gestão da informação que merecia reparos, no momento em que a administração pública grande parte dos seus servidores para trabalhar de casa, geram-se novos riscos que antes não eram mapeados e sem medidas de mitigação claras desenvolvidas previamente, como eventual vazamento de informações que não poderiam ser publicizadas.

Menciona que, em 2020, durante a pandemia, o sistema Fala.br foi divulgado como uma solução para aqueles que ainda não haviam adotado meios digitais de acesso à informação. Cerca de 400 órgãos já aderiram a essa modalidade, sendo utilizado por mais de duas 1.200 unidades de estados e municípios na categoria Ouvidoria.

Versa a respeito da questão da transparência como medida de controle social para políticas públicas que realizam a operação de tratamento de dados. Destaca que é preciso desconstruir a lógica de que o acesso à informação sem transparência serve única e exclusivamente para controle social. A informação é um direito fundamental para o exercício de qualquer tipo de direito. Nesse cenário, a Lei Geral de Proteção de Dados é tida como operacionalização do exercício dos direitos dos titulares de dados.

Deve-se refletir sobre questões culturais que a sociedade brasileira tradicionalmente acabou produzindo e perpetuando ao longo do tempo, principalmente com a percepção de que o Estado poderia ter uma tutela absoluta quase sobre nossa intimidade. No momento em que o cidadão busca um serviço de saúde e busca qualquer tipo de serviço público, ele presta uma série de informações. Isso era visto como uma contrapartida necessária a uma prestação de serviço, de modo que o debate sobre finalidades para o tratamento de dados é essencial.

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

Chama a atenção para a crescente digitalização no cenário do poder público brasileiro, que deve ser acompanhado de uma política clara e ampla de inclusão digital. Hoje o foco está em estratégias de governo digital e digitalização de serviços, mas é necessário também atentar para grupos que são excluídos digitais.

Conclui afirmando que, em um momento no qual se fala em privacidade por desenho de design, é o momento para discutir a transparência por desenho.

Perguntas respondidas e apontamentos finais

BLOCO I

Pergunta feita por Nathan Pascoalini (Delegação do Youth) (presencial):

A pandemia possibilitou o início do uso de tecnologias de rastreamento de contato e esse uso deve perdurar. Neste sentido, houve um caso bem controverso em Singapura em que teve um aplicativo nacional do país, o Trace Together, e os dados coletados foram compartilhados com a polícia local. Considerando esse caso, o contexto da pandemia no Brasil e a relevância da análise do passado para a definição dos passos futuros, o que os participantes pensam sobre o uso destas tecnologias? O que vocês entendem como uma prioridade a ser endereçada no desenvolvimento destas tecnologias?

Pergunta de Marcelo Fornazin (pesquisador da Fiocruz e professor na escola de saúde pública) (presencial):

Em termos de saúde pública, usamos "vigilância" como uma forma de monitorar o desenvolvimento de doenças e fatores de riscos e isso exige muitos dados para que se possa prevenir riscos, organizar campanhas de vacinação, etc. Tenho notado que atualmente meus alunos têm tido dificuldade de acessar dados, que antes eram estudados como dados históricos, uma vez que pela LGPD vários destes dados seriam considerados dados pessoais sensíveis e ainda que seja permitido que autoridades de saúde usem esses dados, esse uso ainda não está muito

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

claro. Questiono se essa questão da vigilância em saúde chegou a ser observada.

Respostas - bloco I:

Dayana Costa - Pondera benefício à população com a proteção de dados e a privacidade. O uso de tecnologias para o atendimento de políticas públicas não pode significar uma ação de vigilância ou de intrusão na esfera pessoal dos indivíduos. A solução apresentada seria garantir a transparência dos procedimentos, além de seguir normas adequadas de proteção para fortalecimento da cultura de proteção de dados. Deste modo, seria possível empoderar o titular e a sociedade para agir frente a abusos e evitar que certas ações sejam implementadas.

Paulo Melo - Menciona a necessidade de ter um olhar crítico para o consentimento. Sem transparência, sem participação pública, e sem a devida expansão da cultura de proteção de dados, há o risco da conformação e surgimento de um cenário autoritário. Há vários casos em outros países de aplicação de tecnologias durante a pandemia que colocam em risco a privacidade ou que têm políticas inadequadas, e não é cabível.

Alessandra Gomes - Retoma os testes feitos na pesquisa que participou, dois apps um do Paraná e outro de Pernambuco geravam QR Code, para que elas apresentassem caso fossem abordadas. Neste QR Code havia o CPF e o horário. A ideia, conforme especulado, provavelmente seria gerar um código de autorização de circulação. Depois de um tempo isso foi retirado das aplicações. Ainda assim, relata que houve outros casos, no Brasil e internacionalmente. O boom de denúncias que chegou aos profissionais de tecnologia fez com que essa questão da rastreabilidade sem intrusão e que ajude políticas públicas. Nesta linha, surgiu a tecnologia da Google (Android), Apple (IOS) e MIT que gerava códigos aleatórios e poderia usar a geolocalização, essa era uma alternativa a ser explorada.

Marcos Lindenmayer - A lealdade tem que ser trabalhada como cultura na administração pública. Vivemos em um mundo em

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

que mais informação parece sempre melhor e, por isso, há tratamentos que são realizados sem finalidade específica. E neste sentido, é necessário ter uma relação de lealdade com o usuário de serviços públicos. A *accountability* é outro ponto essencial, a transparência é um caminho essencial para isso, para permitir o monitoramento por parte da população da proteção de dados. E por fim, a prevenção é muito relevante também para gerir adequadamente as informações.

Sobre a questão do Marcelo, sobre a vigilância em saúde, é necessário lembrar que a melhor maneira de enfrentar essa questão seria ter uma política mais clara sobre como utilizar esses dados no processo de vigilância em saúde. É um processo longo, mas é para onde precisamos caminhar.

BLOCO II

Gabriel Toscano (pelo YouTube):

Qual a opinião dos painelistas com relação à adequação da publicação de dados pessoais no OpenDataSUS, e também se acreditam que a tentativa de anonimização foi eficaz?

Alessandra Gomes - Há uma equipe bem grande trabalhando nisso, a solução ainda não está concretizada, mas há caminhos de anonimização, por criptografia, por algoritmos que não dependem de identificadores individuais. Acredita nessa iniciativa, mas não é algo finalizado.

Dayana Costa - Há uma série de medidas para permitir que a análise não seja prejudicada, sem violar a privacidade. Há muita análise científica a ser feita para aprimorar essas técnicas.

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

DataPrivacyBR Research

Manifestação	Conteúdo	Consenso/Dissenso	Pontos a aprofundar
Posicionamento	Mesmo com a urgência na adoção de tecnologia, é preciso respeitar a privacidade e garantir a proteção de dados pelo poder público	Consenso entre governo, academia, terceiro setor e empresarial.	É preciso pensar para além do acesso a serviços digitais, mas também a inclusão digital de forma democrática
Posicionamento	Dados pessoais são coletados sem o princípio da minimização, muitas vezes sem uma finalidade delimitada	Consenso entre academia e terceiro setor.	Cultura de coleta de dados sem apontar finalidades por parte do poder público brasileiro
Proposta	Fomentar a cultura de proteção de dados centrada na realidade de cidadãs e cidadãos, pensando de forma articulada com movimentos sociais,	Consenso entre academia e terceiro setor	Estratégias de comunicação para cidadãs e cidadãos sobre a proteção de dados pessoais em seu cotidiano

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

	assistência social e direitos sociais		
Posicionamento	Ao realizar o tratamento de dados pessoais é necessário garantir transparência pelo poder público e setor privado	Consenso entre academia, terceiro setor, governo e setor empresarial	O debate sobre a transparência não deve ser centrado na LGPD, e sim na Constituição por ser um direito fundamental

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org