Informações sobre a atividade

Título e tema: Dados pessoais e modernização das investigações criminais no legislativo brasileiro

Proponente: Daniela Eilberg (Pontifícia Universidade Católica do Rio Grande do Sul)

Palestrantes:

- Carina Quito (Carina Quito Advogados)
- Daniela Eilberg (Pontifícia Universidade Católica do Rio Grande do Sul)
- Karen Luise Vilanova Batista de Souza (Tribunal de Justiça do Estado do Rio Grande do Sul)
- Paulo Rená da Silva Santarém (Instituto de Referência em Internet e Sociedade)
- Tiago Misael de Jesus Martins (Ministério Público Federal do Estado da Paraíba)

Moderadora: Eduarda Costa Almeida (Laboratório de Políticas Públicas e Internet)

Relator: Gustavo Ramos Rodrigues (Instituto de Referência em Internet e Sociedade)

Estruturação do workshop

Objetivos e resultados: O ano de 2021 foi marcado por uma intensificação da atividade legislativa de modernização do aparato penal e processual brasileiro frente às novas tecnologias, em especial devido ao crescimento da criminalidade cibernética durante a pandemia. Iniciativas dessa natureza incluem a ratificação nacional da Convenção de Budapeste de 2001, a reforma do Código de Processo Penal, o debate sobre o Anteprojeto de lei de proteção de dados na segurança pública ("LGPD penal"). Tais esforços também são impulsionados por pressões oriundas da seara internacional, onde o debate sobre uma nova convenção referente a cibercrimes se acentua, assim como a controvérsia pública em torno de novos meios probatórios para investigações criminais em ambientes cifrados (client-side scanning, hacking governamental, etc). Esse cenário suscita um necessário debate regulatório com vistas a um equilíbrio entre a busca pela eficiência na persecução criminal e o respeito às garantias fundamentais no século XXI. A fim de contribuir para a referida discussão, o workshop pretendeu proporcionar aos diferentes setores um espaço de reflexão, de construção de consensos e de mapeamento dos dissensos relativos aos riscos e potencialidades das recentes inovações tecnológicas e normativas na persecução penal. Entre as questões específicas a serem abordadas, destacamos: quais os impactos jurídicos, econômicos e sociais das propostas em discussão no Congresso Nacional para os diferentes setores? Que modelos internacionais podem oferecer inspiração para a atualização do arcabouço regulatório referente a direitos digitais e produção de evidências criminais? Como garantir que as propostas em discussão integrem mecanismos de

observância do direito fundamental à proteção de dados pessoais na ausência de uma LGPD penal já promulgada?

O principal resultado pretendido era a construção de entendimentos coletivos multissetoriais a partir de perspectivas diversas sobre novas formas de investigação digital. As falas estruturadas e dúvidas da audiência configuram material de referência para o setor acadêmico, para o jornalismo e mesmo para o poder público, como legislativo e judiciário, para identificar riscos e potencialidades das iniciativas legislativas de modernização das investigações criminais. O painel de composição diversa pôde mapear os consensos e dissensos existentes entre diferentes atores interessados, agrupando argumentos qualificados para tramitação legislativa de textos como o novo Código de Processo Penal e adesão do Brasil à Convenção de Budapeste sobre Cibercrimes.

Justificativa em relação à governança da Internet: O conteúdo do workshop proposto apresenta relação direta com os Princípios para a Governança e Uso da Internet no Brasil afirmados pelo CGI.br. Em especial, sua relevância do tema se evidencia pelos impactos que as propostas legislativas poderão gerar para a realização dos princípios de número 1, 4, 7 e 8 do decálogo. Uma vez que a área penal é onde reside a ação mais intrusiva do Estado sobre os direitos dos cidadãos, o desenvolvimento de parâmetros democráticos alinhados aos padrões internacionais em direitos digitais se revela fundamental para que o princípio da Liberdade, privacidade e direitos humanos seja observado. Do mesmo modo, a eventual aprovação das propostas em debate poderá impactar significativamente os modelos de negócios de provedores de conexão e de aplicação no país, interferindo diretamente no ambiente necessário à efetivação do princípio da inovação. Essa possibilidade é exemplificada pelo texto base da reforma do Código de Processo Penal na Câmara dos Deputados, que pretende alterar o regime de guarda de dados instituído pelo Marco Civil da Internet e compelir provedores de aplicação à decifragem de conteúdos de comunicações privadas veiculados em seus sistemas. Além das repercussões sobre a economia digital e sobre os direitos dos cidadãos, a eventual aprovação de disposições dessa natureza representa um risco aos princípios da inimputabilidade da rede e à funcionalidade, segurança e estabilidade dos sistemas, uma vez que prejudicará a segurança dos usuários e penalizará indevidamente os provedores a fim de combater ilícitos na rede. Tais riscos são agravados pelo cenário de insegurança jurídica ocasionado pela constitucionalização do direito à proteção de dados na ausência de uma LGPD penal, uma vez que as normas relativas à proteção de dados no campo penal não acompanham o paradigma atual da disciplina da proteção de dados. Nesse sentido, resta evidente a importância de um debate plural e tecnicamente maduro acerca do tema proposto para a governança da internet.

Metodologia e formas de participação desenvolvidas durante a atividade: Anteriormente ao evento, foram mobilizadas as redes sociais das instituições parceiras e convidadas a compor a mesa para divulgação do workshop, expondo os pontos de debate e o link para acesso virtual. Nesse momento, também foram coletadas perguntas para entender quais os temas de interesse do público, as quais foram direcionadas para painelistas, a fim de que melhor possam contribuir com o debate. Durante o evento, foi realizada uma thread no Twitter das instituições dos painelistas, relatando em tempo real, de forma resumida, as falas proferidas e principais questões levantadas. Também houve cobertura do evento através de Stories no Instagram, engajando a comunidade interessada em tempo real. O workshop teve formato de mesa redonda, com exposição inicial breve de 5 minutos por parte da moderação, sobre a temática, apresentação da mesa e objetivos pretendidos pelo painel: o debate multisetorial sobre novas formas de investigação criminal. Seguiu-se uma pergunta focada para cada palestrante, com tempo definido de 10 minutos cada. As perguntas orientadoras das exposições foram elaboradas e enviadas aos painelistas anteriormente, considerando as contribuições que cada setor pôde trazer ao debate para evitar sobreposições de falas e permitir maior aproveitamento no evento. Por fim, foram recolhidas perguntas da audiência, com apontamentos das convidadas e convidados.

Síntese dos debates

Síntese dos posicionamentos e propostas apresentadas pelos(as) palestrantes/debatedores e participantes (incluindo as perguntas):

Eduarda Costa Almeida (Laboratório de Políticas Públicas e Internet) iniciou o workshop apresentando o título, o tema e a metodologia do painel. Destacou que o objetivo da atividade seria encontrar um justo equilíbrio entre a garantia dos direitos e liberdades fundamentais e a eficiência e utilidade na persecução penal a partir do exame das propostas em debate no Congresso Nacional, em especial a LGPD penal, a ratificação da Convenção de Budapeste e a reforma do Código de Processo Penal. Notou que a atividade foi um esforço do Grupo de Trabalho sobre Privacidade e Vigilância da Coalizão Direitos na Rede através do Instituto de Referência em Internet e Sociedade (IRIS) e da Associação Data Privacy Brasil de Pesquisa. Em seguida, apresentou os painelistas e passou a palavra para a primeira expositora, Carina Quito.

Exposição de Carina Quito (Carina Quito Advogados)

Pergunta Orientadora: A atualização dos meios probatórios tem estado no cerne da discussão pública sobre a modernização do processo penal brasileiro, em especial a normatização do uso de tecnologias de extração remota de dados (ex: caso Pegasus). Como o recurso a tais ferramentas interage com nosso arcabouço jurídico atual? Que inovações seriam necessárias para que sua eventual utilização observe padrões internacionais de direitos humanos?

A palestrante iniciou sua apresentação destacando sua experiência como advogada criminalista atuante em casos envolvendo quebras de sigilo telemático e ressaltando ser essa a perspectiva que informa sua fala. Quanto à pergunta apresentada, começou por ponderar se tratar essencialmente do uso de tecnologias, desenvolvidas pelo Estado ou adquiridas de empresas privadas, de invasão para o acesso de dados para exploração de vulnerabilidades com fins de persecução penal - uma prática denominada como *hacking governamental* ou *lawful hacking*. Explicou que o Pegasus tem por função essencial invadir celulares e espionar pessoas pelo monitoramento de todas as atividades dos aparelhos alvejados, indo além de acessar as comunicações dos usuários apenas e sem deixar vestígios. Mencionou as denúncias graves sobre a comercialização desse software para governos autoritários e a desvirtuação de seu uso para monitoramento de jornalistas, advogados, ativistas políticos e opositores, o que considerou uma ameaça gravíssima aos direitos humanos.

Ressaltou que são técnicas de investigação substancialmente mais invasivas que quaisquer outras, uma vez que permitem que as autoridades ganhem controle dos dispositivos e possam manipular dados como se fossem dos próprios usuários. Destacou a importância da consciência dos riscos dessas tecnologias para o devido processo, para os direitos humanos e para a segurança dos sistemas. Argumentou que o recurso a essas ferramentas não interage com o arcabouço jurídico atual do direito brasileiro, uma vez que não há previsão legal para esse meio de obtenção de prova e o processo penal se rege pela legalidade estrita, sobretudo no que diz respeito a medidas restritivas de direitos fundamentais. Argumentou que no panorama legislativo atual, o uso dessas tecnologias é inconstitucional e ilegal. Explicou que o arcabouço atual estabelecido por leis como o Marco Civil da Internet, o Código de Processo Penal e a Lei de Interceptações trazem previsões para o acesso a dados cadastrais, registros de conexão, registros de acesso a aplicações de internet, a comunicações eletrônicas armazenadas, a dados em nuvem, para captação ambiental e para interceptações telefônicas e telemáticas. O hacking governamental, no

entanto, difere de todas essas medidas, por mais que as autoridades tentem compará-lo a interceptações, considera que a comparação é impossível em virtude do caráter muito mais excessivo do hacking governamental, que inclusive permite a manipulação dos dados pelas autoridades.

Passando à segunda parte da pergunta, argumentou que deveria haver regulamentação legal do uso dessas tecnologias, preferencialmente precedida de debate amplo e multissetorial sobre o uso da tecnologia e sobre os riscos envolvidos para a sociedade. Pensa também que essa regulamentação legal deve ocorrer da forma mais específica possível, sendo insuficientes previsões genéricas ou nominais para a criação de salvaguardas efetivas ao uso dessas tecnologias. Considera que o texto legal deveria trazer uma disciplina substantiva de procedimento probatório. Deveria haver uma definição jurídica nítida de hacking governamental, quais modalidades seriam adotadas pelo Brasil, condicionar tais medidas a ordem judicial específica e fundamentada, delimitação precisa sobre alvos e definir critérios legais de proporcionalidade estrita e necessidade. Sobre a proporcionalidade estrita, o meio deveria ser reservado apenas a crimes chamados gravíssimos, preferencialmente enumerados taxativamente. Quanto à necessidade, seria adequado que houvesse a indicação de todos os meios utilizados anteriormente utilizados sem sucesso, com indicações das razões pelas quais foram insuficientes para elucidação dos crimes, além da imposição de uma limitação temporal para o uso da medida, que deveria ser a menor possível em razão dos riscos.

Ainda, considera importante criar salvaguardas de transparência e auditabilidade das ferramentas, como o dever de elaborar relatórios de transparência para uma autoridade supervisora. Os relatórios deveriam especificar número de autorizações judiciais concedidas, número de medidas executadas, indicação de quais ferramentas foram utilizadas, de quantos sistemas e dispositivos foram afetados e de quais dados foram coletados. Também considera importante instituir regras para a manutenção de cadeia de custódia, com uma documentação rigorosa sobre os dados coletados, bem como estabelecer prazos legais para a manutenção e eliminação dos dados impertinentes. Além disso, deveriam ser previstos mecanismos de auditoria das ferramentas para assegurar que investigados e réus pudessem questionar a integridade dos dados extraídos e a manutenção da cadeia de custódia.

Reforça os riscos de ferramentas que permitem a manipulação de dados pelas autoridades.

Considera que as adaptações não são poucas e será necessário estabelecer uma regulação detalhada para minimizar os riscos tanto quanto possível, dado o caráter enormemente invasivo e perigoso dessas ferramentas.

Exposição de Daniela Eilberg (Pontifícia Universidade Católica do Rio Grande do Sul)

Pergunta orientadora: o avanço da reforma do Código de Processo Penal no legislativo levantou um debate importante sobre a tutela de dados pessoais na esfera penal na ausência de legislação específica sobre o tema. Dada a constitucionalização da proteção de dados pessoais, que parâmetros devem ser adotados nas investigações criminais a fim de equilibrar a busca pela eficiência e a proteção desse direito fundamental mesmo na ausência de norma específica?

A palestrante iniciou sua fala ressaltando a importância de reformular concepções processuais penais herdadas de uma era analógica e com resquícios de autoritarismo frente à realidade digitalizada, a fim de evitar violações de direitos fundamentais. Reforçou o caráter essencial do direito à proteção de dados a partir da aprovação da PEC 17/19 e como isso nos leva a questionar conceitos e ideias sobre o processo penal.

Notou a importância de articular a dogmática processual penal com a dogmática da proteção de dados para se refletir sobre uma lei de dados pessoais para os fins de segurança pública e persecução penal, como foi o anteprojeto da LGPD penal, e como é necessário abordar toda uma base principiológica tanto no plano do CPP quanto de leis específicas.

Argumentou que embora a LGPD tenha suscitado diversas transformações importantes quanto a questões como prestação de contas e tratamento dos dados pessoais, seu artigo 4º estabeleceu a exceção para a segurança pública e persecução penal, o que demanda uma legislação específica. No entanto, ponderou, a própria exceção determinou que a ANPD receba os relatórios sobre as temáticas excetuadas, evidenciando que existe relação entre a base principiológica da LGPD e as exceções. Assim, a comissão de juristas buscou conectar os princípios já previstos na LGPD, como finalidade, necessidade e transparência a requisitos específicos da matéria penal, como o princípio da reserva legal.

Argumentou que a sensibilidade específica do tratamento de dados no campo penal decorre do caráter coercitivo do tratamento de dados, o que demanda bases legais que respaldem o tratamento para além do consentimento, respeitando balizas de proteção ideal, de autodeterminação informacional e de atenção com relação às finalidades do tratamento, às reservas legais e parlamentares, e às normas autorizativas de intervenção informacional. Destacou o princípio da separação informacional, isto é, que toda a intervenção em direitos fundamentais durante o ciclo de vida dos dados não deve estar sob o controle de uma única autoridade. Notou que o reconhecimento da autodeterminação informacional e da integridade dos sistemas informáticos não apenas protege o livre desenvolvimento da personalidade, mas propicia a contenção de uma série de práticas vigilantistas.

Reforçou ser importante evidenciar não apenas os princípios da LGPD, como também os da reserva de lei, do devido processo informacional e do devido processo penal, bem como pensar na responsabilização e prestação de contas, na transparência e na accountability e na separação dos poderes informacionais. Somente desse modo, seria possível dar conta da complexidade suscitada pelas novas formas de investigação criminal, sobretudo quanto aos riscos para direitos fundamentais. Notou que há autores, como Tercio Sampaio Ferraz Junior, que destacam ser imprescindível vencer conceitos obsoletos e repensá-los a partir de um raciocínio probatório que dê conta das diversas formas de dados presentes na realidade hoje. Por exemplo, seria importante superar previsões baseadas na lógica de dados estáticos, a fim de ter métodos menos intrusivos quando de uma ordem judicial para franquear o acesso à prova digital.

Por fim, considerou essencial que compreendamos que como o direito à proteção de dados, a inviolabilidade da intimidade e da vida privada e o sigilo das comunicações no contexto das quebras de sigilo e interceptações telemáticas. Considerou o conceito de proteção de dados como essencial para pensar como endereçar questões tecnológicas e pensar numa estrutura normativa capaz de atender às lacunas atuais na segurança pública brasileira, a exemplo da ausência de diálogo interinstitucional, sob risco de uma transparência deficitária. Notou que as novas tecnologias não alteram somente os métodos de policiamento e investigação, mas reacendem discussões no próprio campo da proteção de dados. Concluiu destacando a importância do diálogo interdisciplinar.

Exposição de Karen Luise Vilanova Batista de Souza (Tribunal de Justiça do Estado do Rio Grande do Sul)

Pergunta orientadora: Em que pese a ausência de uma norma específica, a principiologia da Lei Geral de Proteção de Dados Pessoais teve algum impacto sobre algum aspecto prático no tratamento dos dados pessoais experimentado no dia a dia do seu trabalho à frente da Vara do Júri? Algum relato de caso real envolvendo tratamento inadequado de dados pessoais de um indivíduo ou de algum grupo social poderia demonstrar a importância de serem adotados cuidados diferentes por parte do poder público, advogados ou Ministério Público?

A palestrante iniciou sua fala contextualizando sua experiência enquanto juíza de direito, que trabalhou durante 18 anos no interior do estado do RS e está há quatro anos titular do tribunal do júri da comarca de Porto Alegre, voltada ao exercício da jurisdição criminal. Também trabalha como formadora da Escola Nacional de Formação de Magistrados, onde trabalha com as disciplinas de questões raciais e proteção de

vulneráveis. Ponderou que o trabalho com essas questões por vezes envolve situações de violência letal, o que provoca reflexões sobre a persecução penal e os julgamentos.

Explicou que buscaria apresentar o que se tem de concreto no Poder Judiciário, em especial no contexto gaúcho, a respeito da temática de proteção de dados pessoais nos processos criminais. Notou que a promulgação da LGPD foi seguida pela Recomendação 73/2020 do CNJ para que fossem criados grupos de trabalho em todos os tribunais do país para discussão da lei e de sua aplicação. No RS, esse processo foi seguido pelo Ato 27/2020 do TJRS, para que tais questões fossem debatidas e examinadas. Mais recentemente, houve também a Resolução 363 de 12/01/2021.

Nesse período, constatou que o Poder Judiciário se dedicou a criar comitês gestores e editar um plano de trabalho para a implementação da lei, pensar em políticas institucionais para a proteção de dados, conhecer as realidades e conteúdos da lei, bem como criar um fórum interinstitucional para o compartilhamento de experiências. Notou que esse fórum demonstra a dificuldade para o enfrentamento da questão, embora se trate de questões envolvendo direitos fundamentais de acesso à informação e privacidade dos indivíduos.

Asseverou que o ato normativo mais concreto que observou no TJRS subsequentemente aos diversos fóruns e palestras foi a edição do provimento 20/22, que alterou a consolidação normativa judicial para proibir a prestação de dados pessoais por telefone e determinar que a pesquisa de processos criminais para o público externo a partir do nome da parte fosse facultada apenas à própria parte, aos advogados e demais atores processuais. Considerou a redação da segunda parte peculiar, uma vez que essa restrição implica que a pesquisa não é facultada ao público externo.

Ao mesmo tempo, o acesso pelos advogados e demais atores processuais gera um impacto potencial sobre a presunção de inocência, por isso sempre foi bastante restritiva ao conceder o acesso a dados processuais penais a advogados e demais atores. Afirmou compreender que se o advogado não tem procuração nos autos, não há motivo para requerer o acesso a certas informações. Assim, considera necessária a demonstração do interesse mediante peticionamento para que somente então seja facultado ao advogado o acerto a dados como nome, CPF, filiação e outros dados importantes, a menos que seu conteúdo seja sigiloso.

Destacou que todos os essenciais à realização da justiça, inclusive a advocacia, a Defensoria Pública, o Ministério Público e a magistratura, vivem o dilema de tentar compreender qual direito fundamental está em jogo nas discussões e no acesso a determinados dados. Direitos associados ao tema incluem acesso à informação, privacidade, segredo de justiça, e afins. E a avaliação de quais dados podem ser objeto de acesso ao público em geral, a jornalistas e a advogados, é necessário trabalhar com o

princípio da proporcionalidade. No Tribunal Europeu, há um teste tripartite: a medida que interfere na privacidade do indivíduo deve ser adequada, necessária e gerar benefícios para o andamento do processo.

No Tribunal do Júri, a apuração dos fatos por vezes envolve o acesso ao conteúdo dos dispositivos dos indivíduos e/ou de suas redes sociais e esse acesso por vezes ocorre de forma questionável. Também trabalha-se muito com as interceptações telefônicas e quebras de sigilo, que devem ser mediante autorização judicial, mas ponderou que por vezes tais dados chegam ao processo com a informação de que foi o próprio réu, a parte ou o investigado envolvido no crime que autorizou o acesso amplo e irrestrito ao seu equipamento. Isso geralmente é seguido por um pedido de extração de dados.

Considerou que esse ponto é importante, porém ainda é pouco discutido entre os atores envolvidos no processo penal. Em diálogos prévios com seus colegas sobre a lei e com relação à proteção de dados, notou que de modo geral havia uma percepção de que o tema não havia sido tratado previamente por eles. E esse dado, essa ausência de tratamento sobre o tema, é especialmente relevante porque no Tribunal do Júri as questões consideradas são aquelas que envolvem mortes violentas que recaem sobre um segmento populacional específico. Há um número expressivo de mortes violentas de jovens negros e há o encarceramento em massa da população negra, então na medida em que há um esforço atual de pensar a proteção de dados na esfera penal, é preciso se questionar para quem servirá a proteção de dados. Para essa população, que é a principal atingida pela violência letal e pelo encarceramento, ela não serve até hoje.

Exposição de Paulo Renã da Silva Santarém (Instituto de Referência em Internet e Sociedade)

Pergunta orientadora: Quais os potenciais riscos ou vantagens da adesão do Brasil à Convenção de Budapeste para a proteção de dados pessoais nas investigações criminais? E em que medida a norma internacional pode repercutir nos debates sobre a LGPD Penal?

O palestrante iniciou comentando que iria contextualizar sobre os desenvolvimentos legislativos recentes que levaram à adesão do Brasil à Convenção de Budapeste sobre o Cibercrime. Ela é um tratado internacional assinado em 2001 no âmbito do Conselho da Europa, uma organização francamente desconhecida do senso comum brasileiro. Ouve-se muito falar da União Europeia, mas pouco do Conselho, que é uma organização com mais países que fez a norma com o objetivo de uniformizar os conceitos, procedimentos e tipos penais relativos aos crimes cibernéticos. Trata-se de uma ideia com benefícios, mas cujo

exercício da soberania brasileira levou a uma opção de não-adesão às normas que não participou da elaboração.

Notou que o Brasil não foi sequer tradicionalmente convidado a aderir à convenção. Refletiu que houve um esforço de realizar uma adesão aos conteúdos da convenção sem o procedimento convencional de ratificação durante o debate sobre a Lei Azeredo. Isso seria feito pela cópia de partes da convenção e enquadramento desses dispositivos como se fossem meras partes de um projeto de lei ordinária. Tais dispositivos foram suprimidos da versão final aprovada do projeto, que inseriu o artigo 154-A no Código Penal.

O Ministério Público, por meio do MRE, passou a incidir no ambiente europeu para obter um convite para o Brasil, que foi encaminhado em dezembro de 2019. Considerou que o processo iniciado desde então ocorreu praticamente sem debate e num processo legislativo excessivamente célere e muito questionável, dada a ausência de sessões presenciais no congresso nacional. Recordou que a palestrante Daniela participou da única audiência realizada no parlamento sobre o tema e foi a única voz dissonante, dado que os demais participantes teceram inúmeros elogios à adesão sem qualquer crítica ou análise detida.

Ponderou que há dispositivos na convenção que demandam declarações e reservas por parte dos países que fazem a adesão. Explicou que esses mecanismos permitem diferentes formas de adesão, porém a resposta brasileira foi uma adesão à integralidade do documento. Notou que a Coalizão Direitos na Rede buscou mobilizar parlamentares contra essa adesão acrítica e sugeriu que fossem feitas declarações para três dispositivos e reservas sobre quatro dispositivos referentes a questões sobre como certos tipos penais deveriam ser interpretados, exigindo, por exemplo, que sempre houvesse dolo para a caracterização de certas condutas tipificadas - como é a regra no Brasil -, bem como sobre garantias e salvaguardas investigativas.

Quanto aos riscos, argumentou que a adesão ao texto genérico da convenção impõe o risco de uma interpretação reduzida das garantias existentes em nosso ordenamento, dado que o Brasil passa a ter um compromisso internacional com um texto menos protetivo dos direitos processuais. Assim, é possível que se enfraqueçam as proteções vigentes no ordenamento. Outro risco seria que normas que ainda estão em debate poderiam ter seu andamento prejudicado e a promulgação de novas garantias fosse impactada pela adesão.

Conjecturou que alguns magistrados e magistradas teriam a sensibilidade para garantir tais direitos e assegurar que a produção probatória e a cadeia de custódia sejam respeitadas, porém outros serão menos protetivos e potencialmente temerários nesses processos, gerando inclusive insegurança jurídica sobre resultados que poderiam ter sua legalidade e constitucionalidade questionadas em instâncias superiores. Isso poderia gerar nulidades processuais penais em razão de condução indevida.

Quanto às vantagens, notou que a convenção exige limitações e parâmetros legalmente previstos como condições e salvaguardas para sua própria aplicação. Assim, ao exigir condução adequada e proporcionalidade na aplicação de suas medidas de persecução, isso poderia suscitar um exame das lacunas presentes no arcabouço legislativo hoje vigente. Tal revisão poderia levar a uma incrementação do presente ferramental normativo nacional.

Por fim, destacou que a LGPD poderia ser o espaço adequado para a realização do debate de forma mais adequada, sem esquecer que a reforma do Código de Processo Penal também apresenta diversos dispositivos referentes a salvaguardas e garantias sobre dados pessoais e direitos fundamentais. No entanto, destacou que a inércia da LGPD penal é sintomática de uma incongruência entre a importância dessas mudanças e a atenção dada a elas no momento brasileiro atual.

Considerou que não se trata necessariamente de uma urgência, dado que o país acaba de sair de uma pandemia e pode ter outras prioridades de mérito, porém ponderou que o retorno à vida presencial pode propiciar condições mais adequadas a esse debate. No entanto, afirmou esperar que o país possa encontrar nos debates sobre LGPD penal e a reforma do CPP, as soluções para os problemas que o processo legislativo apressado, superficial e pouco debatido que a adesão à Convenção de Budapeste trouxe.

Exposição de Tiago Misael de Jesus Martins (Ministério Público Federal do Estado da Paraíba)

Pergunta orientadora: Um dos grandes fatores propulsores do debate sobre a modernização das investigações criminais no país tem sido o crescimento da criminalidade cibernética nos últimos anos, sobretudo na pandemia. Quais os principais desafios enfrentados pelo MPF na persecução penal relativa a esses casos? Em que medida nosso arcabouço normativo presente está apto à lida com os cibercrimes? O que poderia melhorar?

O palestrante iniciou ressaltando a importância de enriquecer o debate apresentando contribuições com uma perspectiva de avaliação diferente daquela trazida pelos demais expositores. Destacou que é membro do grupo de apoio sobre criminalidade cibernética do MPF, que encaminhou uma das notas técnicas encaminhadas ao Congresso Nacional em defesa da ratificação da Convenção de Budapeste pelo Brasil. Argumentou que a Convenção já é conhecida há duas décadas, por isso houve tempo para que o tema fosse adequadamente debatido e estudado, e que há dois protocolos adicionais. Entre outras, essas considerações contribuíram para convencer o MPF a defender a ratificação da Convenção.

Continuou identificando premissas que considera inafastáveis no debate sobre produção de provas e investigações criminais. A primeira é de que o Estado tem o dever de investigar, processar e punir crimes, obrigação que decorre do direito fundamental à segurança e do monopólio estatal do uso legítimo da força e se efetiva através do sistema de justiça. O corolário dessa premissa é que as investigações por vezes se deparam com dados pessoais, sensíveis ou não, e dados sigilosos - nos termos da LGPD penal. Quando isso ocorre, o direito fundamental à proteção de dados deve ser observado.

A segunda premissa é que quando dois direitos fundamentais, como segurança e privacidade, colidem, cabe ao legislador ponderar os dois e dispor sobre o tema, como na disciplina das técnicas de investigação e parâmetros de tratamento de dados pessoais. No caso da proteção de dados, a LGPD estabeleceu exceções para as finalidades de segurança pública e persecução penal, indicando a necessidade de legislação específica sobre o tema, que deve observar medidas proporcionais e estritamente necessárias ao atendimento do interesse público. Afirmou que é do interesse do MPF que o APL seja protocolado para que as questões sejam levadas ao fórum adequado, que é o poder legislativo.

Expressou que há críticas profundas ao APL, como a exigência de informações sobre dados em fase anterior ao recebimento desses dados, que seria um ponto inexplicável. Considerou que o APL estabelece exigências sobre os órgãos de investigação que essas instituições não têm condições de atender no primeiro momento da investigação. Entendeu que a falta de experiência com investigações influenciou negativamente a elaboração do APL.

A terceira premissa é de que as técnicas de investigação variam de acordo com a complexidade do crime. Para fins didáticos, pode-se estabelecer uma distinção entre duas categorias de técnicas de investigação.

As técnicas tradicionais de investigação incluem apreensão de objetos e instrumentos (art. 6º, II, CPP); oitiva de ofendido, testemunhas e investigado (art. 6º, IV e V, e arts. 185 e 225, CPP); reconhecimento de pessoas ou coisas e acareações (art. 6º, VI, e arts. 226 a 230, CPP); exame de corpo de delito e qualquer outra perícia, inclusive perícia de TI (art. 6º, VI, e arts. 158 a 184, CPP); reconstituição de crimes (art. 7º, CPP); requisição de dados e informações cadastrais (dados de base) de vítima ou suspeito a órgãos públicos ou empresas privadas (art. 13-A, CPP; arts. 15 a 17, Lei das ORCRIM; e art. 10, §3º, MCI); prova documental (arts. 231 a 238, CPP); busca e apreensão domiciliar (arts. 240 a 250, CPP). Destacou que a perícia de TI, requisição de dados e informações cadastrais e a busca e apreensão domiciliar são especialmente relevantes para a matéria em debate.

Ao lado das técnicas tradicionais, haveria técnicas especiais, regradas fora do CPP. Estas incluem a colaboração premiada, (arts. 4º a 7º, LEI ORCRIM); captação ambiental de

sinais eletromagnéticos, ópticos ou acústicos (art. 8º-A, Lei 9296/96); ação controlada (arts. 8º e 9º, Lei ORCRIM); Acesso a dados telefônicos (art. 3º, IV, Lei ORCRIM e art. 4º, V, Lei 9472/97); acesso a dados telemáticos (art. 7º, III, e art. 10, 2º, MCI): dados de conteúdo, tráfego e metadados (ex: geofencing); interceptação das comunicações telefônicas (art. 1º, Lei 9296/96); interceptação das comunicações telemáticas (art. 1º, parágrafo único, lei 9296/96), com decisão judicial indicando meio de execução (art. 4º e 5º); afastamento do sigilo financeiro (LC n. 105/01); afastamento do sigilo fiscal (art. 198, §1º, I, CTN); infiltração policial física e virtual (arts. 10 a 14, Lei ORCRIM; e 190-A e 190-E, ECA) - limites definidos na decisão judicial.

Das técnicas especiais, destacam-se a captação ambiental, o acesso a dados telemáticos (inclusive dados de conteúdo e metadados), a interceptação das comunicações telemáticas, bem como a infiltração policial virtual, cujos limites são dados em decisão judicial.

Ao comparar as técnicas de investigação presentes em nosso ordenamento com aquelas dispostas na Convenção de Budapeste, manifestou desacordo com a avaliação de que o Brasil buscou se adequar à Convenção de Budapeste mediante lei ordinária, pois há institutos jurídicos equivalentes no ordenamento brasileiro que foram sendo desenvolvidos antes da adesão à Convenção. Exemplos incluem a conservação expedita de dados informáticos armazenados e dados de tráfego (art. 16 e 17, CB), equivalentes às ordens de preservação de dados (art. 13, 2º e art. 15, 2º, MCI); a ordem de injunção (art. 18, CB), equivalente à requisição de dados cadastrais (art. 10, 3º, MCI) e quebra telemática (art. 10, 1º, MCI); busca e apreensão de dados informáticos armazenados (art. 19, CB), equivalente à quebra telemática para a busca remota (art. 7º, III, art. 10, 2º e art. 22, MCI) e busca e apreensão domiciliar para a busca presencial (arts. 240 a 250, CPP); recolha em tempo real de dados relativos a tráfego e conteúdo (arts. 20 e 21, CB), equivalentes à interceptação telemática (art. 1º, parágrafo único, Lei 9296/96). Defendeu que o único instituto constante na Convenção e ausente no cenário brasileiro seria a divulgação parcial de dados de tráfego. Todas as outras estariam previstas em lei.

A quarta premissa é de que as técnicas de investigação por vezes são operacionalizadas por tecnologias desenvolvidas pelo Estado ou por atores privados. Exatos incluiriam o sistema de movimentação bancária (SIMBA), o de movimentação de dados telefônicos (SITTEL), de dados fiscais (SIFISCO) o Guardião/Sombra para interceptações telefônica, os portais de law enforcement dos provedores de aplicação, ferramentas de rastreio de criptoativos, de cruzamento de vínculos e o emprego de *malwares*, inclusive *spyware*.

Ressaltou que existem diversos outros tipos de malware e spyware que não o Pegasus, os quais podem ser aplicados em seu lugar, portanto não seria verdade que todo

tipo de malware modificará os dados existentes no dispositivo. Tal funcionalidade existe no Pegasus, mas não significa que seja comum a todo e qualquer malware empregável. Considera que não existe nenhum empecilho de natureza legal para o emprego de tecnologias dessa natureza na investigação. Identifica quatro efeitos que podem ser alcançados com malware: 1) interceptação de comunicações telemáticas; 2) ativação de câmera e microfone; 3) obtenção de dados armazenados no dispositivo sem o conhecimento do investigado; 4) modificação de dados. As três primeiras funcionalidades seriam adequadas à investigação, pois a interceptação telemática estaria prevista em lei, com salvaguardas e garantias previstas no próprio texto legal. Uma vez que a lei não dispõe sobre a tecnologia que deve ser empregada, a representação pela interceptação é que deve definir o tema, sendo esta controlada judicialmente. Qualquer tipo de tecnologia pode ser utilizada na interceptação telemática, dado que a ordem judicial deve definir o meio de interceptação. A ativação de câmera e microfone, por sua vez, equivale à captação ambiental. O artigo 8-A da Lei das interceptações dispõe sobre o tema, determinando que a ordem judicial disporá sobre o meio de captação. Assim sendo, não há impedimento para o uso dessa tecnologia, dada a neutralidade tecnológica da lei.

A quinta premissa é de que os dados recebidos devem obedecer à cadeia de custódia. A sexta premissa é de que a tecnologia pode dificultar a atividade investigativa a exemplo da criptografia como padrão (Going Dark problem), a rede TOR, o uso de criptoativos para pagamentos em contextos de organizações criminosas. Embora lícitas, tais tecnologias atrapalham a investigação.

A sétima premissa é que ferramentas tecnológicas podem ser empregadas ilegalmente por agentes do Estado e atores privados. Exemplos incluem *hacking* governamental (controle de mensagens, causação de dano e vigilância), ciberespionagem e caso Cambridge Analytica. O corolário dessa premissa é que o Estado não pode investigar ilegalmente sob pena de imprestabilidade da prova e responsabilidade do agente.

A oitava e última premissa é de que os dados coletados pelo Estado são apenas uma pequena parte dos dados coletados por empresas privadas destinatárias das ordens judiciais. O corolário dessa premissa é de que a ameaça principal à privacidade decorre da coleta massiva de dados por empresas privadas, no exercício de seus modelos de negócios voltados para publicidade e modelagem comportamental. Defendeu que esse cenário é muito mais gravoso que a coleta estatal no âmbito de investigações criminais legalmente regradas e judicialmente controladas.

Concluiu argumentando que é dever do Estado, na realização do direito fundamental à segurança, realizar uma investigação cada vez mais tecnológica para processar criminosos e punir crimes cada vez mais tecnológicos, respeitando os direitos fundamentais dos investigados, dentre os quais a proteção de seus dados pessoais.

Pergunta 01 (Natane Santos): Existem diversas legislações nacionais e internacionais que repudiam o racismo em todas as suas formas e um dever nacional e internacional de combate ao racismo, porém na prática opera um genocídio contra os povos preto e indígena e as tecnologias também têm sido usadas como parte desse genocídio, mesmo porque não existe tecnologia neutra. No AqualtuneLab, do qual é co-fundadora, dedicam-se à reflexão sobre o potencial discriminatório das tecnologias. Perguntou sobre a importância de disposições expressas sobre um compromisso antirracista na LGPD penal, entedendo o antirracismo não somente como uma palavra da moda, pois o termo tem sido usado como uma palavra da moda, enquanto o Brasil permanece como um país anti-negros. Destacou sua atuação prévia com as mães de maio, a Rede Manguinhos, dentre outras organizações e coletivos e que existem pesquisas e relatórios sobre o tema. Isso também é uma questão para as investigações criminais, pois é difícil demonstrar a presunção de inocência de alguns corpos, os quais têm cor, e há um movimento de criminalização de ativistas de direitos humanos.

Pergunta 02 (Thiago Moraes): Recentemente foi aberta a assinatura do segundo protocolo da Convenção de Budapeste, que traz uma série de salvaguardas para a proteção de dados. Por ser um protocolo, não é obrigatório. Os painelistas veem a possibilidade do protocolo reacender o debate para que as salvaguardas sejam trazidas em algum momento, possivelmente na LGPD penal?

Pergunta 03 (Pedro George de Brito): No RS, as varas criminais já estão sob a égide do processo judicial eletrônico e se o SEEU está sendo utilizado pelo processo de arbitramento das penas, dado que esses sistemas permitem vasculhar os processos mesmo para as pessoas que estão como usuários externos, além de MP, defensoria, advogados em si. Há preocupações com o zelo em relação aos dados pessoais dos processos, dado que há magistrados que não tem tanto zelo. Como pensar isso nacionalmente? Pois há uma tendência a se pensar localmente e os Poderes Judiciários vão criando suas condições e não há uma política nacional de preservação dos dados. O que podemos ajudar a fazer?

Resposta de Paulo Renâ da Silva Santarém (Instituto de Referência em Internet e Sociedade):

Iniciou respondendo à pergunta de Thiago, notando que será necessário debater o primeiro protocolo, que trata de questões envolvendo racismo. Agradeceu às contribuições de Natane, que considerou muito pertinentes e pouco debatidas. Em diálogo com a

exposição de Tiago, ponderou que o dever estatal de garantia da segurança pública também é acompanhado pelo dever de seguir a lei. Em uma alegoria, sugeriu que seria inadmissível, por exemplo, uma “tortura que respeitasse os direitos humanos”, pois isso seria uma contradição em termos. Similarmente, o tratamento dos dados deveria ser respeitoso desde o início, não sendo possível entender que um tratamento contaminado desde o início teria seus eventuais danos resolvidos pela destruição subsequente dos dados. Exemplificou com o tratamento indevido do então juiz Sérgio Moro com a ligação telefônica da então presidenta Dilma Rousseff para o ex-presidente Lula da Silva. Concordou que não pode empregar os dados de tráfego em qualquer caso. Questionou sobre as razões do Brasil não ter feito ressalvas na adesão à convenção quanto aos dados de tráfego, cujo acesso poderia ser admitido somente em casos envolvendo crimes de punição com reclusão (ou apenas detenção). Do mesmo modo, ainda não foi indicado ninguém para representar o Brasil na participação de uma rede contínua de troca de dados de investigações criminais, ainda está indefinido se será a ANPD, o CNJ, o Ministério da Justiça, etc. Quanto à diferença entre o Estado e o Google, ressaltou que há diferenças basilares que chamam atenção especial para os riscos da vigilância estatal, como o fato de o Google não ser uma república e não ter poder de sanção. Considerou que o Estado não ajuda a exigir mais respeito aos dados quando pretende avançar sem a devida proteção no tratamento desses dados.

Resposta de Karen Luise Vilanova Batista de Souza (Tribunal de Justiça do Estado do Rio Grande do Sul)

Agradeceu pela manifestação de Natane. Considerou que todos da mesa poderiam contribuir, pois a luta antirracista não deve partir somente da população negra. Recordou que o APL da LGPD penal tem uma previsão ou consideração de não-discriminação. Notou que desde o caso Beto, ocorrido no Rio Grande do Sul, foi criada uma comissão de juristas para revisão de toda a legislação brasileira para torná-la antirracista, na qual trabalhou na parte criminal e dos direitos sociais. Algumas contribuições foram realizadas nessa comissão para tratar sobre o reconhecimento pessoal, crimes de injúria racial, entre outras situações envolvendo a esfera criminal. Sugeriu que houvesse proporcionalidade na composição dos jurados no Tribunal do Júri. As sugestões da comissão estão sendo incorporadas paulatinamente aos projetos de lei. No caso específico do APL, considerou necessário que haja uma mobilização da sociedade civil e de todos os atores do direito para que a questão especifica do antirracismo seja reafirmada nessa legislação quando ela estiver em debate, a fim de que se construam mecanismos para evitar que uma parcela da

população permaneça subjulgada - ainda que haja 134 anos da abolição da escravidão no país.

Quanto à pergunta do Pedro, relatou que no RS trabalha-se com o E-Proc e que poucos colegas utilizam o SEEU. Acredita que é possível trabalhar com a questão no nível nacional e que as recomendações do CNJ tem sido muito frutíferas para a demonstração do caráter nacional da magistratura e que devem existir políticas judiciárias específicas para tratar de determinadas questões, inclusive que deem conta efetivamente da proteção de dados. Ocorreu que uma das preocupações é com relação aos indivíduos que cumprem a sua pena e, ainda que peçam a reabilitação, seus dados permanecem armazenados e podem ser utilizados para que se formule convicções sobre sua vida, comportamento ou eventual prática de outros crimes - embora, com relação àquele fato, já tenham cumprido sua dívida com a sociedade. Considerou que o CNJ é um espaço existencial frutífero, que tem tratado muitas questões com resultados úteis. Concluiu dizendo que o CNJ, por intermédio do Observatório de Direitos Humanos, tem ouvido as mulheres que são vítimas indiretas dos crimes praticados contra a juventude e determinou que todos os tribunais do país tenham centros de atenção às vítimas nas maiores cidades, para que possam saber seus direitos.

Identificação de consensos, pontos a aprofundar e dissensos:

Tipo de manifestação (posicionamento ou proposta)	**Conteúdo**	**Consenso ou Dissenso**	**Pontos a aprofundar**
Posicionamento	O uso de tecnologias de extração remota oculta de dados, como o Pegasus, é inconstitucional e ilegal no direito brasileiro atual	Dissenso	Aplicação do princípio da legalidade estrita ao uso

			de tecnologias invasivas na investigação criminal
Posicionamento	O uso do hacking governamental via ferramentas de invasão não é comparável a interceptações telefônicas e telemáticas	Dissenso	Definição do conceito de hacking governamental
Posicionamento	É fundamental pensar o processo penal a partir de um filtro do direito constitucional		Interação entre o direito fundamental à proteção de dados e a dogmática processual penal
Posicionamento	A sensibilidade específica do tratamento de dados no campo penal decorre do caráter coercitivo do tratamento de dados		
Posicionamento	É preciso superar o conceito de dados estáticos, que está obsoleto		
Posicionamento	O acesso de advogados que não possuem procuração nos autos a dados pessoais processuais penais demanda justificação mediante demonstração de interesse		
Posicionamento	É preciso se questionar para quem servirá a proteção de dados pessoais, pois ela não tem atendido à população negra e vítima de violência policial		Juridicidade das autorizações de acesso amplo e

			irrestrito aos dispositivos das pessoas investigadas
Posicionamento	A adesão brasileira à Convenção de Budapeste está sendo excessivamente célere, pouco participativa e democrática	Dissenso	Avaliação sobre a de ressalvas na adesão brasileira
Posicionamento	A adesão à íntegra da Convenção de Budapeste impõe o risco de uma interpretação reduzida das garantias existentes em nosso ordenamento		
Posicionamento	O APL da LGPD Penal estabelece exigências sobre os órgãos de investigação que essas instituições não têm condições de atender no primeiro momento da investigação		Exigência de informações sobre dados em etapa anterior à coleta desses dados
Posicionamento	Há institutos jurídicos equivalentes aos previstos na Convenção de Budapeste no ordenamento brasileiro sobre investigações criminais		
Posicionamento	Qualquer tipo de tecnologia pode ser utilizado na interceptação telemática e na captação ambiental, dado que a ordem judicial deve definir o meio	Dissenso	Interação entre neutralidade tecnológica e princípio da legalidade estrita

Posicionamento	A principal ameaça à privacidade decorre da coleta massiva de dados por empresas privadas, no exercício de seus modelos de negócios voltados para publicidade e modelagem comportamental e não da coleta estatal no âmbito de investigações criminais.	Dissenso	