Painel: TICs, Dados e Segurança Pública
Manaus, 04 de outubro de 2019.

DADOS GERAIS SOBRE O PAINEL

- Proponente

ARTIGO 19 BRASIL - Terceiro Setor.

- Palestrantes ou debatedores(as)

Jacqueline Abreu, Universidade de São Paulo (USP), Comunidade Científica e Tecnológica.
Advogada e doutoranda em Direito pela Universidade de São Paulo.

José Soares Guerrero, FullFace, Setor Empresarial.
Chief Technology Officer (CTO) da FullFace Biometric Solutions.

Rodrigo Leite Prado, Ministério Público Federal (MPF), Setor Governamental.
Procurador da República em Minas Gerais, membro do Grupo de Apoio ao Combate de Crimes Cibernéticos e dos Grupos de Trabalho sobre Crimes Financeiros e sobre Cautelares Reais do MPF.

Veridiana Alimonti, Electronic Frontier Foundation (EFF), Terceiro Setor.
Advogada, trabalhou no Idec (Instituto Brasileiro de Defesa do Consumidor) e é membra do Intervozes. É coordenadora da EFF para a América Latina.

- Moderador
Paulo José Lara, ARTIGO 19 BRASIL, Terceiro Setor.
Sociólogo e Cientista Político, é assessor de direitos digitais da ARTIGO 19 BRASIL.

- Relatora
Rafaela Alcântara, ARTIGO 19 BRASIL, Terceiro Setor.

INFORMAÇÕES SOBRE O PAINEL

1. Resumo

Nos últimos meses, o Brasil vivenciou uma série de iniciativas de uso de tecnologias de vigilância para combater práticas criminosas, como a implantação de câmeras no Carnaval do Rio de Janeiro e a ativação do Centro Integrado de Inteligência de Segurança Pública no Paraná, tornando-se evidente o protagonismo das TICs dentro dos órgãos de segurança pública. Nesse sentido, a sessão visou debater, tendo em vista tal contexto, os impactos da utilização de aparatos de vigilância para liberdade de expressão.

2. Objetivos e resultados

O workshop reuniu profissionais de diferentes locais do país, setores da economia e áreas de atuação para discutir a utilização de tecnologias de vigilância pelo setor público -- como reconhecimento facial, coleta de DNA e quebra do sigilo das comunicações -- para fins de segurança pública e

persecução criminal. Nesse contexto, a sessão tratou de duas questões principais centrais na discussão.

A primeira referiu-se aos impactos desse tipo de tecnologia na condução de investigações e persecuções criminais, bem como a consequência de seu uso massivo por parte de autoridades públicas de segurança pública para os direitos à intimidade, vida privada, sigilo das comunicações e proteção de dados. Dentro desta primeira questão, também debateu-se sobre o impacto da massificação dos aparatos de vigilância possibilitados pelas tecnologias de comunicação e informação para a liberdade de expressão e de reivindicação de direitos por parte de movimentos sociais e grupos políticos. Nesse sentido, abordou-se ainda os projetos de lei que têm o potencial de causar impacto na relação entre repressão, persecução criminal e TICs.

A segunda reflexão colocada pela sessão disse respeito à importância de existência de mecanismos de transparência, prestação de contas e auditoria satisfatórios para a utilização dessas tecnologias por autoridades policiais e órgãos de segurança pública. Nesse contexto, a proposta objetivou ouvir as percepções tidas pelos diferentes setores presentes na mesa de debate quanto ao atual cenário de transparência em relação à implementação de aparatos de vigilância para combate ao crime. Mais especificamente, foi levada à discussão o entendimento jurisprudencial dos Tribunais Superiores brasileiros no tocante à apreensão de dispositivos móveis e os impactos e limites das tecnologias de reconhecimento facial.

Além disso, a sessão também objetivou a disseminação deste debate no ecossistema de governança da Internet no Brasil para que indivíduos de diferentes regiões e setores pudessem estar inteirados do estado da arte da referida discussão no país.

Como resultado, notamos que o workshop proporcionou uma visão bastante ampla sobre o tema, tanto no sentido de abordagem temática quanto sob a perspectiva multissetorial. Tivemos visões e perspectivas de membro do Ministério Público Federal atuante na área criminal; de uma integrante do Terceiro Setor que trabalha na Electronic Frontier Foundation, organização internacional que atua com privacidade digital, liberdade de expressão e inovação; uma pesquisadora acadêmica que trouxe uma abordagem sobre as teses jurídicas referentes à apreensão de dispositivos móveis pelas forças de segurança em diferentes contextos fáticos; além do representante do setor privado que compartilhou a visão sobre biometria facial desde sua experiência no meio empresarial. É válido destacar ainda que o público participante com perguntas trouxe provocações igualmente de bastante relevância.

Pontos de consenso significativos foram identificados e, de maneira muito relevante, pontos a aprofundar foram levantados, o que é de extrema importância quando se trata de assuntos que estão na ordem do dia e que têm o potencial de impactar cotidianamente a vida em sociedade.

3. Justificativa em relação à governança da Internet

Nos últimos meses, o Brasil presenciou a elaboração de uma série de iniciativas para aumento do uso dos aparatos de vigilância baseados em tecnologias da informação e comunicação por parte de organismos da segurança pública e do poder legislativo para combate ao crime. No Carnaval de 2019, por exemplo,

foram instaladas câmeras com tecnologia de reconhecimento facial para identificação de criminosos nas ruas do Rio de Janeiro. Ainda em âmbito administrativo, houve a inauguração do Centro Integrado de Inteligência de Segurança Pública Regional Sul em Curitiba no mês de maio, que visa à integração de estratégias de inteligência de treze órgãos de segurança pública e de mais de 70 bases de dados disponibilizados pelas agências participantes.

Já na esfera legislativa, o Congresso Nacional conta atualmente com 19 projetos em tramitação que visam a combater práticas terroristas no país, dentre os quais 6 são referentes ao ano de 2019, sendo que a maioria deles objetiva a flexibilização das garantias constitucionais para agravamento das medidas punitivas e permissão para utilização de aparatos de violação do sigilo das comunicações. Além disso, o Pacote Anticrime, recentemente proposto pelo atual Ministro da Justiça, contém diversos dispositivos que objetivam à utilização de medidas tecnológicas para a identificação de indivíduos, interceptação telefônica e quebra do sigilo de dados. Tendo em vista este contexto, é evidente a importância do presente debate para a Governança da Internet, tendo em vista tanto as questões relativas aos direitos individuais dos cidadãos, como a privacidade e a liberdade de expressão, quanto debates mais amplos sobre transparência, prestação de contas e responsabilidade por parte do setor público.

4. Metodologia

O moderador realizou uma breve explanação sobre a conjuntura do tema, passando depois a palavra a cada debatedor/a que, por sua vez, trouxe uma visão específica sobre os aspectos discutidos, durante um tempo mais longo, para que pudessem articular seus conhecimentos sobre os recortes do assunto que se propuseram a abordar. Depois o debate se voltou a escutar considerações do público e, ao final, mais uma vez foi dada a palavra para os debatedores, a fim de que eles pudessem responder e dialogar com as questões trazidas pela plateia.

5. Síntese dos debates

O Moderador, Paulo José Lara, apresentou o tema da mesa e também a organização da sociedade civil propositora da mesa, a Associação ARTIGO 19 BRASIL, que atua pela defesa da liberdade de expressão e do acesso à informação, e vem trabalhando há algum tempo com a questão da intersecção entre tecnologias digitais e segurança pública. Destacou ainda que recentemente tem havido uma série de proposições legislativas visando modificar a relação entre tecnologias digitais e a maneira pela qual as forças de segurança vêm se utilizando delas.

Nesse contexto, apontou ainda que isso traz o debate sobre questões como quebra de criptografia de comunicações - e, como resultado, acesso a dispositivos móveis, aquisição de dados biométricos e genéticos pelas forças de segurança e Estado, reconhecimento facial. Citou ainda a Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei n. 13.709/2018, que recentemente foi aprovada e que também está relacionada a questões como base de dados, troca de informação, tratamento de dados para investigação criminal e contratos para entes privados e públicos no universo da segurança pública.

Adicionalmente, explanou um pouco sobre o formato do painel, compartilhando

que apresentaria os debatedores antes de cada um/a falar, mas a ideia seria a que fossem apresentadas duas questões para iniciar o debate - estas seriam comentadas pelos convidados e depois seria aberta a palavra ao público.

Dr. Rodrigo Prado e Veridiana Alimonti se propuseram a comentar sobre o impacto da tecnologia na persecução penal e na propositura de leis e regulamentos. Além disso, falariam ainda sobre qual o estado atual da utilização de dados e o que se propõe atualmente em matéria de legislativa sobre o tema.

O moderador apresentou ainda o estudo da ARTIGO 19 BRASIL sobre os Projetos de Lei que buscam a alteração da Lei Antiterrorismo - Lei n. 13.260/2016. A organização elaborou um infográfico sobre riscos, questões que precisam ser levadas em consideração e pensadas que estão propostas nos projetos; e que, nesse contexto, possam de alguma forma apresentar riscos ameaças violações aos direitos humanos e à liberdade de expressão.

Tendo essa questão como norte, passou a palavra a Dr. Rodrigo Prado.

Dr. Rodrigo Prado, para introduzir o tema, falou dos conceitos, a fim de situar os presentes, dentro dos atores da segurança pública, como Inteligência; patrulhamento ostensivo; persecução e repressão criminal.

Segundo Dr. Rodrigo, a ele parecia que o impacto das novas TICs na persecução criminal seria menor do que se imagina. Isso porque o Código de Processo Penal (CPP) é de 1941, quando a projeção de duração de um inquérito policial era de 30 dias. Aquele contexto em que o CPP foi pensado é diferente do que temos hoje. Aponta que hoje o tempo é consideravelmente mais longo - exemplifica dizendo que em Minas Gerais, a Polícia Federal não consegue instaurar um inquérito em menos de 90 dias, que dificilmente são relatados em menos de 3 ou 4 anos. Aponta ainda o grande número de inquéritos e ações penais que se desenvolvem ao mesmo tempo. Alude ainda que são muitas bases de dados, mas que quase nunca são usadas, porque não são interoperáveis, tanto porque os sistemas costumam ser instáveis e também por conta da falta de pessoal.

Apontou ainda que, na repressão penal, o reconhecimento facial serve normalmente ao cumprimento de mandados de prisão em aberto e à produção de provas. E, como ele enseja o monitoramento indiscriminado de um número de pessoas indeterminável, acaba sendo uma técnica muito controversa já banida em muitas partes do mundo, até mesmo por gerar falsos positivos que refletem o preconceito com grupos vulneráveis e identificam muito mais mulheres negras do que homens brancos como possíveis autores de crimes. Alude ainda que até onde tem notícia o reconhecimento facial não é disciplinado ainda no direito brasileiro, mas já constitui realidade no patrulhamento ostensivo em mais de 30 cidades. Na opinião pessoal de Dr. Rodrigo, ele deveria ser autorizado apenas em casos concretos em que fosse demonstrada a proporcionalidade e a vantagem do sacrifício do direito à privacidade das pessoas. Por exemplo: quando são explodidos terminais nas salas de autoatendimento da Caixa Econômica Federal que são explodidos terminais, as câmeras de circuitos fechados gravam a cena e, ainda que se veja a pessoa, não se sabe como ela é. O índice de solução dessas ocorrências é muito baixo no Brasil e, nesse caso, seria uma possibilidade a se pensar a implementação, preferencialmente mediante decisão judicial, de um mecanismo de vigilância a partir reconhecimento facial.

Dr. Rodrigo explana ainda que o confronto de impressões digitais é uma realidade comum, corrente na justiça criminal, e que poderia ser melhor explorada se não houvesse 27 bancos nesse sentido no País (um para cada estado). Essa situação tende a mudar em breve pq a Lei n. 13.444/2017 criou a Identificação Civil Nacional, mediante a integração das bases de dados do TSE, da polícia federal no que diz respeito à emissão de passaportes, dos Detrans e Cartórios de registro civil. O risco à privacidade surge nesse contexto, a seu ver, à medida em que os estados passaram a coletar outros dados biométricos que não a impressão digital, como dados sobre íris, padrão de face, padrão de voz, isso na esteira do Pacote Anticrime apresentado pelo Ministério da Justiça. Isso ajudaria os atores da persecução penal, mas não se pode deixar de reconhecer que isso gera pro Estado uma possibilidade de abuso muito grande, na medida em que sabendo a voz e a face de alguém, ele pode identificar a pessoa em qualquer lugar e monitorar as atividades dela a qualquer momento.

Mencionou ainda que o banco de dados genético, criado via legal no Brasil, restringe a coleta aos casos de necessidade imperiosa para a investigação reconhecida por decisão judicial e condenados pela prática de crimes hediondos e crimes dolosos e violentos. Aduz que se trata de um potencial muito grande cuja legitimidade já foi reconhecida por decisões do Tribunal Europeu de Direitos Humanos e que aqui no Brasil é subutilizada em razão da nossa barreira tecnológica e de investimento. Hoje em dia o banco nacional de perfil tem cerca de de 30 mil perfis genéticos cadastrados, quase todos coletados em cenas de crimes, no corpo de vítimas de crimes sexuais, de restos mortais, e não identificados a uma pessoa específica. nesse contexto, a utilidade do banco ficaria comprometida, comprometendo também a punibilidade de crimes sexuais e de crimes violentos em que normalmente há rastros de sangue e suor na cena do crime.

Expôs ainda que as demais TICs citadas pelo moderador, como o acesso a dispositivos e a quebra de criptografia, parecem atender a outra demanda da justiça criminal, a luta contra crimes de colarinho branco, sobretudo aqueles crimes praticados através de pessoas jurídicas em que é necessário reunir um volume muito grande de dados, na tentativa de comprovar algumas circunstâncias pouco tangíveis em comparação com crimes pouco violentos - desde conversas até verificação de onde possuem bens no exterior. São situações em que o Estado é hipossuficiente na relação processual, são crimes cujos seus agentes têm assessoria técnica para não deixar rastros, lavam o produto do crime, se representam por bancas de advocacia grandes, é necessária cooperação internacional. Defende que essa prova é muito cara para eles - provas que antes eram obtidas por busca e apreensão, hoje em dia costumam estar armazenadas em meio digital.

Explica ainda que o acesso à dispositivos têm obedecido a uma lógica de “gato e rato” no Brasil, em que os criminosos costumam estar à frente da persecução criminal. Nesse sentido surgiu a Lei de Interceptações Telefônicas - Lei n. 9.296, em 1996, todos migraram para o Blackberry, que na época ainda não podia ser interceptado. A Polícia Federal fez um convênio com a administradora do Blackberry e em seguida passaram a utilizar dispositivos como Skype, Voip e e-mails em servidores próprios e não em servidores que atendiam a ordens judiciais, a informação sobre a prática do crime passou a ser armazenada em nuvem. Levou-se muitos anos para conseguirem ter acesso às nuvens e hoje em dia praticamente só se conversa por meio de aplicativos de mensagem instantânea.

Dr. Rodrigo finalmente ainda levanta que, com isso, a criptografia de ponta a ponta virou objeto da principal discussão sobre investigação no mundo. Trata-se de um tema extremamente difícil. De um lado, porque a inacessibilidade a esses dados tem feito com que o Estado use de meios cada vez mais invasivos, como a inoculação de vírus nos celulares e uso interceptação física.

A palavra então volta ao moderador e Paulo José afirma que sabemos que há critérios importantes, parâmetros utilizados. Porém vemos no brasil que para além dessa importância toda, iniciativas legislativas vêm sendo propostas muitas vezes colocando para o público soluções para a questão da segurança pública. Passa então a palavra para Veridiana Alimonti.

Veridiana Alimonti se apresenta rapidamente e explica que a EFF, onde trabalha, é uma organização que atua também com discussões da proporcionalidade do uso de dados para investigações. Explica que é bastante sabido e debatido que nossas atividades cotidianas, atividades políticas, comunicações emitem uma série de informações sobre nós, sobre nossas atividades. Essa emissão contínua interfere na liberdade de expressão e em outros direitos como a liberdade de associação, de reunião etc. Por exemplo: a geolocalização fornecida pelo celular que pode dizer onde a pessoa estava em um protesto. Nesse sentido, a privacidade é uma zona que diz respeito a outros direitos. São impactos não só individuais, mas também coletivos, inclusive em relação à própria segurança. Por isso, o acesso a essa profusão de dados pelas autoridades de investigação deveria respeitar preceitos de necessidade e proporcionalidade, porque senão estaríamos sujeitos a uma série de abusos e ao desrespeito a uma série de garantias.

Afirma ainda ser necessário significa que tem que ser o meio menos gravoso para atingir o fim legítimo da investigação. Deve ser proporcional ao levar em consideração o impacto a outros direitos nesse balanço, tendo em vista que muitas vezes dizem respeito a dados pessoais sensíveis. A legislação atual de diversas maneiras busca atender a essas exigências. Cita como exemplos: requisitos para interceptação de telecomunicações na Lei de Interceptações Telefônicas; necessidade de ordem judicial prévia e outros requisitos para acessar registro de conexão e acesso à aplicação previstas no Marco Civil da Internet - Lei n. 12.965/2014; hipóteses restritas de acesso a perfil genético, como Dr. Rodrigo mencionou, a condenados por crimes graves de acordo com a Lei de Execução Penal - Lei n. 7.210/1984.

Afirma ainda que, como Paulo mencionou na pergunta, temos um conjunto de projetos de lei que buscam afrouxar essas garantias de forma bastante perigosa. Ela fala que vem acompanhando o Pacote Anticrime e os Projetos de Lei (PLs) presentes no infográfico elaborado pela ARTIGO 19, mas deve haver muito mais. Menciona ainda que surgem muitos projetos, sendo difícil acompanhá-los. Veridiana passa a destacar alguns pontos dos PLs que julgam importantes.

Menciona, nesse contexto, que alguns pretendem acessar metadados (dados sobre a comunicação), registros de comunicação e acesso à aplicação, em geral nos PLs isso diz respeito aos registros de chamadas e de conexão e acesso à aplicação. Isso sem ordem judicial prévia, que é uma garantia muito importante da lei. O PL 1595, por exemplo, permitiria acesso direto junto às empresas.

Afirma ainda que tradicionalmente a inviolabilidade das comunicações era muito relacionado ao conteúdo das comunicações. Porém, hoje, as comunicações são

parte da vida diária; tudo o que fazemos gera dados. Assim, o registro de com quem você falou, quando em que com que frequência, os sites que vc acessou — tudo isso diz muito mais do que o remetente e o destinatário de uma carta, por exemplo. E diz muito sobre cada um de nós, muito mais que a comunicação em si.

Acessar metadados sem autorização judicial, vai na contramão do que a Corte Interamericana de Direitos Humanos se manifestou no caso Escher x Brasil sobre interceptação ilegal de cooperativas de trabalhadores rurais ligadas ao Movimento dos Trabalhadores Rurais sem Terra - MST. A Corte reconheceu que os metadados deveriam estar protegidos pela inviolabilidade das comunicações privadas e, assim, seria necessária uma autorização judicial para que a autoridade competente tenha acesso. Isso é visto em outras legislações além da brasileira. Esta garantia está presente, por exemplo, nas legislações espanhola, argentina e chilena.

Outro ponto dos PLs é o que se chama de infiltração virtual. Nesse sentido, o Pacote Anticrime e o PL 9.808, vão para além do que prevê o Estatuto da Criança e do Adolescente (ECA), que possui a previsão legal de infiltração de agentes na internet no caso de crimes específicos. É característico da infiltração, nesse contexto, o ganho da confiança da organização criminosa ou de quem está sendo investigado, para que se possa ter acesso às informações que a investigação busca. E o ECA cria a modalidade de infiltração virtual para que o agente se infiltre/ganhe a confiança em grupos de comunicação, por exemplo. Porém existem projetos de lei que querem expandir esse instituto para obrigar a colaboração de empresas de Internet para, por exemplo, inserirem um participante invisível em uma conversa privada sem que outros participantes da comunicação saibam. Isso pode parecer uma ideia razoável, a princípio, mas isso compromete a integridade e a segurança das comunicações de todos que utilizam essa comunicação, e não só o alvo da comunicação. Implementar uma proposta como essa implica em modificar o código dessas aplicações e os mecanismos de autenticação das partes da comunicação dos quais elas se utilizam - mecanismos que é fundamental para que os participantes tenham certeza de que eles estão falando com o destinatário correto. Mensageiros com criptografia de ponta a ponta (como o Signal e o WhatsApp, por exemplo) se utilizaram de uma técnica de criptografia de chave pública, em que cada dispositivo gera um par, uma chave, uma delas é pública, para que qualquer pessoa possa cifrar a mensagem para quem ela vai mandar. Mas a mensagem cifrada só vai poder ser aberta pela chave privada da pessoa pra quem ela está enviando a mensagem.

Afirma que por isso a autenticação seria importante. Porque um dos maiores desafios é você autenticar que tem a chave pública correta da pessoa com a qual vc quer se comunicar. Caso contrário, atores maliciosos poderiam criar uma chave pública falsa para determinado destinatário, e como consequência a mensagem cifrada poderia ser lida pelo ator malicioso. Alterar esses mecanismos para tornar essas comunicações menos confiáveis coloca em risco a comunicação de todo mundo que se utiliza dessas aplicações, como jornalistas e suas fontes, ativistas, policiais no curso de investigações sigilosas, advogados e seus clientes.

Além disso, a autenticação ainda seria um desafio da segurança de sistemas, que ainda exige pesquisas e investimentos. Assim, se uma lei passa a exigir que os mecanismos sejam mais frouxos, na verdade o que tende a acontecer é que

os investimentos e pesquisas nisso também tendem a ser desincentivados. Esse é só um dos problemas que se relacionam com o debate de sempre em relação à exigência do que chamamos de “porta dos fundos” ou “acesso excepcional em comunicações criptografadas”. De forma geral, elas envolvem mudanças no código, no software dessas aplicações, que são mudanças complexas que podem ampliar a vulnerabilidade a ataques que os próprios desenvolvedores desconhecem.

Uma forma comum de lidar com isso é justamente fazer aplicações de código aberto em que a própria comunidade técnica pode verificar a segurança dessas aplicações. Mas se aplicação tiver um mecanismo de acesso excepcional inserido isso não vai ser aberto e o escrutínio da comunidade técnica será comprometido.

Um ponto que coloca em questão a adequação desse tipo de medida que altera o código de todos que utilizam é que sempre haverá (como o exemplo do Blackberry) possibilidades fora da jurisdição brasileira de aplicações que não tenham essas vulnerabilidades, ou mesmo aplicações de código aberto que organizações criminosas com financiamento podem até recriar para terem elas as comunicações seguras e os usuários comuns ficarão eles com as aplicações que terão vulnerabilidades maiores, por conta desse tipo de colaboração. A proporcionalidade também tem que ser levada em consideração, porque se está criando uma vulnerabilidade que atinge todos que utilizam dessa aplicação e não somente a pessoa que está sendo investigada. Embora se possa ter um algo específico e pedir uma chave numa decisão judicial, mas para que a empresa possa entregar, ela já teve que mudar o seu código e pode ter criado uma vulnerabilidade, enfraquecendo seu sistema de autenticação para todos/as.

Veridiana aponta ainda a questão dos dados biométricos. Afirma que, como Dr. Rodrigo já havia comentado, hoje, pela Lei de Execução Penal, para que seja coletado o perfil genético, tem que ser um condenado, por crime praticado dolosamente, com violência grave contra pessoa, ou qualquer dos crimes previstos no art. 1º da Lei de Crimes Hediondos. Pela proposta do Pacote Anticrime, qualquer condenado por crime praticado com dolo, mesmo antes do trânsito em julgado da decisão condenatória, seriam submetidos obrigatoriamente à identificação do perfil genético. Segundo o PL correspondente, caso eles se negasse, isso seria condenado falta grave na execução penal.

Destaca ainda que a prática como é hoje já é alvo de questionamento no STF, por haver o entendimento de que consiste em produção de provas contra si mesmo, o que contrariaria dispositivo constitucional. Além disso, a lei hoje determina que a exclusão do perfil genético do banco de dados deve ocorrer no prazo determinado em lei para prescrição do delito. Pelo Pacote Anticrime, a exclusão é quando ocorre a absolvição ou em caso de 20 anos depois do cumprimento da pena. Nesse contexto, Veridiana questiona: qual a proporcionalidade disso?

No GT de Penal foi aprovada uma emenda que melhora a proposta, mas terá que passar pelo plenário da Câmara, pelo Senado etc. Além disso, há no Pacote Anticrime o banco nacional multibiométrico e de impressão digital. Ele tem como objetivo armazenar dados biométricos, de impressões digitais e quando possível íris, face e voz para subsidiar investigações criminais federais estaduais ou distritais. São previstas hipóteses bastante amplas de integração e interoperação de bancos de dados, sem considerações sobre a necessidade específica de

coleta e interoperação para uma investigação específica. sem considerações sobre o respeito à finalidade inicial da coleta, segurança do armazenamento ou controle de registros, de acesso e utilização desse sistema, por exemplo.

Afirma que parece muito prático ter todos esses dados biométricos de todo mundo, Mas eles são marcadores únicos, que identificam ou verificam a identidade de pessoas, que usam características físicas ou comportamentais intrínsecas e são considerados dados mais propensos a consequências e usos discriminatórios. No caso do DNA, ele contém uma grande quantidade de informação pessoal sensível, com o potencial de revelar detalhes intensamente privados sobre a vida e o futuro de uma pessoa, incluindo com quem ela está relacionada, a sua propensão a doenças, e possivelmente até suas tendências comportamentais. Embora seja uma técnica importante, também podem ocorrer erros; ela não está imune a erros.

Menciona que em 2015, por exemplo, o San Francisco Chronicle revelou que um analista de laboratório criminal estava fazendo suposições sobre evidências genéticas incompletas e de baixa qualidade, tendo vinculado falsamente um perfil de DNA ao réu de um caso. Então é preciso que haja procedimentos e que a necessidade e a proporcionalidade sempre estejam presentes. Falhas também podem ocorrer em sistemas de reconhecimento facial, como Dr. Rodrigo já falou, seja com falsos negativos, seja com falsos positivos, vimos um caso recente no Brasil. Por isso a importância de considerações quanto à necessidade de coleta e tratamento, medidas de segurança e de controle no acesso e utilização desses dados, e um debate com especialistas e com a sociedade para que a utilização desses sistemas não se dê de forma abusiva e em desrespeito a garantias fundamentais. Isso se agrava mais com a possibilidade de tratamento e decisões automatizadas que busquem utilizar esses dados para prever pessoas com mais probabilidade de cometer crimes, reincidir, desenvolver comportamento desviante etc e, considerando a seletividade do sistema penal, a coleta, o acesso e o tratamento desses dados tende a aprofundar a estigmatização de grupos vulneráveis como a população negra. Por fim, Veridiana ressalta ainda que, considerando que o veto correspondente não foi derrubado na LGPD, ainda há a questão de como se conseguirá fazer a revisão por pessoal natural de decisão automatizada.

O moderador compartilha então que agora passamos para a segunda parte do painel. Na primeira houve um panorama geral sobre segurança pública e tecnologia e agora será um debate um pouco mais específico, trazendo a abordagem sobre dois temas: dispositivos móveis e reconhecimento facial. Paulo José traz ainda uma questão provocadora, no sentido de aprofundar sobre como essas tecnologias estão sendo utilizadas nas situações concretas e pensar em como se consegue desvendar os mecanismos possíveis de transparência, os procedimentos ligados à aplicação dessas tecnologias e como vem sendo a relação entre o poder público e como os entes privados vêm respondendo a essas questões.

Nesse momento, Jacqueline Abreu começa a abordar o tema dos celulares e investigações criminais; ela é doutoranda pela USP e compartilha ainda que grande parte de sua fala é reflexo da pesquisa que desenvolveu no InternetLab.

Aduz que quando nossa Constituição Federal de 1988 (CF88) foi promulgada, os telefones começaram a se tornar populares e hoje estamos transitando da telefonia fixa para a telefonia móvel de uma maneira que quase todo cidadão

tem esse dispositivo. Nesse contexto, menciona ainda artigo que desenvolveu que aborda como ocorreu em expansão da vigilância (em capacidade e volume de armazenamento) em decorrência de o ordenamento jurídico não responder em igual medida à evolução tecnológica.

Jacqueline ainda trouxe dados sobre aumento significativo de dispositivos móveis e, voltando à CF88, menciona o art. 5º, inciso XII, em que é preservado um nível de sigilo de comunicação como regra. Menciona nesse contexto a exceção, regulamentada pela Lei n. 9.296/1996, a qual determina que se houver um indício concreto de autoria ou participação de alguém em um crime punível por reclusão e aquela prova for necessária e não puder ser coletada de outra maneira, será autorizado excepcionalmente que as autoridades de investigação interceptem comunicações telefônicas. Ressalta ainda que, em 1988, tinha-se em mente os telefones, que não deixam registros, pois as pessoas se comunicavam em tempo real.

Cita ainda que surgiu uma jurisprudência no STF, no âmbito do HC 91.867/PA, de abril de 2012, que entende que esse inciso XII do art. 5º só abarca comunicações que estão em fluxo, comunicações enquanto elas ocorrem, em tempo real, e que seria esse o escopo da Lei n. 9296/1996. Nesse caso concreto, a polícia apreendeu um celular, analisou o histórico de chamadas do dispositivo celular e assim pode apurar diversas informações do indivíduo. O caso foi ao STF porque o defensor desse caso tentava encabeçar a tese de que essa prova seria ilícita e portanto não poderia ser utilizada para incriminar o acusado naquele caso.

O STF considerou - com voto condutor de Gilmar Mendes - que não haveria diferença entre papéis que a pessoa tivesse no bolso e o celular que ela carregava. E considerou que pelo art. 6º do Código de Processo Penal, é dever da polícia apreender objetos com relação ao fato e colher todas as provas, uma vez que tenha conhecimento de uma prática de infração penal.

Jacqueline alude ainda que talvez a analogia de papéis que se carrega no bolso não correspondem mais aos celulares que temos hoje em dia. Naquele caso, estavam em jogo as capacidades de um celular de 2004. A polícia hoje, se apreende um celular, tem acesso a uma infinidade de dados e não somente ao registro do histórico de chamadas. Que regras então devem ser postas ou que tipo de reconsideração deve ser feita na interpretação do STF nessas novas condições? Essa é a pergunta fundamental.

Expôs ainda uma pesquisa empírica sobre julgados de tribunais estaduais no Brasil sobre o tipo de argumentação que se utiliza para considerar prova lícita ou ilícita que é obtida pelo acesso a celular numa situação de flagrante. Em geral, a jurisprudência em todo País, tem considerado que a polícia pode sim acessar o celular, sem ordem judicial, isso porque supostamente o art. 5º, inciso XII, não protegeria as informações armazenadas, mas sim somente as informações em fluxo.

O Superior Tribunal de Justiça, por sua vez, no HC 51531/RO proferiu três votos de três ministros diferentes alinhados na mesma noção de que hoje “o celular deixou de apenas ser um instrumento de conversação pela voz à longa distância, permitindo, diante do avanço tecnológico, o acesso de múltiplas funções”. Nesse contexto, afirma que há o entendimento de que quando a polícia tem acesso ao celular, isso representa um impacto muito maior ao cidadão.

Jacqueline cita ainda o HC 168.052, mais recente, que aborda a mesma situação fática: celular apreendido em uma situação de flagrante. O ministro Gilmar Mendes se manifestou no sentido de que deve ser levado em conta que desde então os celulares mudaram bastante, sinalizando que tecnologias mudaram e que hoje se tem acesso muito grande a informações pessoais por meio de celulares e isso deve ser levado em conta, devendo haver uma autorização judicial prévia para que esses celulares sejam acessados.

Ainda sobre o assunto, Jacqueline faz uma provocação, sobre existir uma ficção de que com ordem judicial se resolverá tudo, que se houver a exigência de ordem judicial, estaremos protegidos. Nesse contexto, ela afirma que para conseguir ordem judicial não é tão difícil assim, a depender do juiz. Então, parece que tem-se que aprofundar as discussões a respeito dos requisitos materiais (e não somente requisitos formais, caso da ordem judicial). Porque, por exemplo, se a pessoa utilizou um celular para agredir alguém, não é necessário acessar o conteúdo do celular para processar a pessoa. A depender do crime, não se precisa ter acesso ao conteúdo, ou se poderá recortar o período de tempo a se acessar no celular. Isso deve estar refletido nas ordens judiciais e no requerimentos de policiais. importante se levar a privacidade a sério também nesses termos materiais e, nesse sentido, aprofundar o debate.

Jacqueline traz ainda outra hipótese, aquela em que o celular foi deixado na cena do crime, mas a pessoa não estava lá e a polícia quer identificar a pessoa. Cita, nesse contexto, um caso de STF com repercussão geral - de relatoria do Ministro Dias Toffoli, o ARE 1.042.075. Nesse contexto, Jacqueline aponta que é muito mais difícil defender o mesmo nível de proteção à privacidade se uma coisa foi largada em um lugar, diante das doutrinas do direito - apesar de ser possível e ela defender a privacidade. Defende que será muito melhor se o caso citado anteriormente for resolvido antes, porque será mais fácil construir uma jurisprudência positiva para proteção a dados em si, e não somente a dados em fluxo.

Cita ainda outro caso: e se o acesso tiver sido com ordem judicial, a polícia também tiver acesso a comunicações futuras? Por exemplo: a polícia apreendeu o celular e fez a sincronização com o Whatsapp Web. a polícia devolveu o celular à pessoa e mandou ela embora, havendo o espelhamento do aplicativo e a polícia tendo acesso ao histórico de mensagens pelo Whatsapp Web, podendo ainda podia escrever e acompanhar em tempo real ao que a pessoa estava escrevendo, até pelo menos a sincronização acabar.

No caso do HC 99.735, o STJ considerou ilegal a prova – sendo uma medida de obtenção de prova híbrida. Havia acesso a dados armazenados, ao mesmo tempo em que houve uma interceptação e ainda se ganhou a capacidade de editar o conteúdo. Esse tipo de medida não comportaria analogia com nenhuma outra e necessitaria de uma regulamentação específica. Esse raciocínio seria importante por fazer alusão à necessidade de uma previsão legal. Afirma que as polícias ao redor do Brasil seriam muito criativas - e é importante que haja essa questão da previsão legal, para que se possa efetivamente haver segurança sobre o que se pode ser feito ou não em relação à atuação dessas polícias.

Fez alusão ainda ao que Dr. Rodrigo falou sobre a apuração do fato criminoso em diferenciação das atividades preventivas. Achou interessante que ele abordou essas diferentes da atividades e atores dentro da lógica na persecução criminal. Isso porque a lógica é distinta existe um regramento extenso de direito

processual penal e em outras normas que regulam o procedimento de quebra de sigilo, que regulamenta o que a polícia pode fazer ou não. A lógica da atuação preventiva é diferente; não há suspeita concreta contra alguém de cometimento ou participação em crime punível com reclusão, só se está fazendo o policiamento ostensivo. Nesse contexto, Jacqueline traz o questionamento: qual o critério para poder fazer ou não algo que implique uma restrição à privacidade?

Finalmente, a pesquisadora ainda mencionou casos de acesso a celulares no contexto de policiamento ostensivo nas ruas. A pessoa é parada em uma abordagem e o policial pede acesso ao celular - isso ocorre muito no Brasil sob a lógica muitas vezes de um consentimento, pois a pessoa não teria se oposto. Nesse sentido, levantou a pergunta: como na prática tentamos coibir que isso aconteça, já que nesse caso não há um indício concreto contra alguém? Já que não se poderia acessar o celular daquela pessoa, como no dia a dia impedimos que o direito constitucional seja violado? Ainda nesse âmbito, mencionou que encontrou na Internet relatos bastante negativos de reações que pessoas teriam enfrentado ao se negar a entregar o celular à polícia nesse tipo de abordagem.

De volta ao moderador, Paulo José menciona que relaciona a fala de Jacqueline alude à questão do acesso às TICs de pessoas pertencentes a grupos mais marginalizados - em especial considerando os recortes de raça e classe. Ato contínuo, passa a palavra, ao representante do setor empresarial José Guerrero.

Em primeiro lugar, José Guerrero alude sempre observar essas questões sob uma ótica técnica, e não jurídica. Afirma que, em especial na área em que ele atua, de biometria e reconhecimento facial, um ponto é importante é a questão que hoje existe da generalização do uso de biometria facial. Menciona generalização porque as pessoas se acostumaram com a tecnologia, estão utilizando ela e não têm noção da extensão desse uso. A informação que guardada no smartphone não está exatamente ali, ela pode estar sendo guardada em qualquer outro lugar. E esse armazenamento, mesmo não sendo qualificado, pode levar à identificação positiva de um indivíduo. Assim, com uso de biometria facial no smartphone, haveria o potencial de se ser identificado em qualquer lugar do mundo.

Afirma que uma premissa básica no desenvolvimento dos projetos de tecnologia seria a preservação de informação e a ética em relação ao uso da informação que se está coletando. Menciona que se fala muito também é o uso discriminatório; mulheres e negros teriam uma taxa de reconhecimento muito baixa. Segundo José, realmente há isso, mas depende da tecnologia que está sendo utilizada. Os modelos em que foram identificados os problemas de reconhecimento seriam modelos antigos e genéricos, os quais tratam a população como massa e não como indivíduos. Nesse contexto, afirma que as pessoas negras e as mulheres realmente terão uma dificuldade maior na questão do reconhecimento, com um número de falsos positivos muito maior. Isso porque a grande massa utilizada como modelo seria a massa masculina e ariana. Ou, no caso da China, masculina e asiática.

Compartilha que as empresas que fazem reconhecimento facial na China não conseguem sair do território chinês - porque o modelo deles todos partem de uma premissa genérica e não numa premissa de indivíduo único. Então quando eles vão para países com características europeias ou americanas, ou quando vêm para países com a miscigenação como o nosso, não conseguiriam

reconhecer as pessoas, por conta do modelo que foi utilizado. Então uma das premissas disso é tratar o modelo de biometria facial de forma individualizada, guardando características de indivíduo e não características relativas a nação, raça e etnia. Isso é uma coisa que eles aplicariam desde o início do desenvolvimento do projeto, que é preservar essas características individuais e não trabalhar dentro do modelo massificado.

Afirma ainda que existem hoje mais 200 fornecedores de serviços tecnologia facial, porém desenvolvedores de tecnologia para o mercado são apenas nove. E, desses nove, pelo menos sete deles utilizam modelos generalizados, o tal modelo de massificação. Menciona como uma questão interessante, principalmente nesse aspecto, considerando modelos de aprendizado e modelos de treinamento desse sistema, é a questão de utilização de sistemas de reconhecimento facial em espaços públicos. Destaca que é importante pensar no quanto isso é importante, o quanto isso interfere na individualidade de cada um na preservação de informação e qual o benefício que isso traz.

Segundo José, se observarmos sob a ótica de segurança pública, o benefício seria muito grande Porém, se for utilizado na segurança pública sem ter a fiscalização da sociedade civil, porque isso pelo potencial de se tornar um problema muito grande, uma vez que se começa a interferir no direito de ir e vir do cidadão. Enquanto se estaria capturando aquela informação do cidadão, não qualificando e utilizando-a só para compará-la com uma base de indivíduos foragidos ou procurados pela justiça, José Guerrero acha válido; o problema que pode acontecer, segundo ele, é a qualificação e individualização dessa informação. Isso já aconteceu em algumas cidades dos EUA - por isso que começaram a tirar os sistemas de vigilancia publica de lá. Assim, o indivíduo capturado por um sistema de segurança pública, em algum instante foi qualificado e identificado, mesmo sem ele ter alguma passagem ou algum problema que justificasse essa qualificação. Segundo José, trata-se de um problema grave, em relação ao qual a sociedade civil tem que ter mecanismos de acompanhamento e vigilância, porque senão estaremos em um grande “Big Brother”. Afirma que como hoje o celular já diz onde estaremos e captura nossa face, temos que ajustar isso à não corrupção dos nossos direitos individuais, a sociedade civil tem que encontrar maneiras de cobrar a não qualificação das informações das pessoas.

José Guerrero se posiciona ainda no sentido de que se teria que montar grupos de discussão com técnicos, juristas e órgãos de controle, para tentar formar um colegiado e discutir essas questões, que, na sua opinião, ainda são mal discutidas no Brasil. Afirma ainda que na Europa se avançou bastante nesse aspecto até a criação da General Protection Data Regulation - GPDR, que seria bem interessante, com artigos específicos referentes à biometria facial, fora os artigos sobre biometria, preservando muito o direito individual e dado não qualificado.

Segundo o debatedor, um ponto muito importante é a transparência contratual - a partir do instante que ele é fornecedor de tecnologia para um órgão público, ele teria que ter transparência nas ações e deixar claro onde e como as informações estão armazenadas, fornecendo ao cidadão o direito de solicitar a exclusão e verificação dessas informações. Segundo ele, a sociedade civil deve ter acesso não só via órgão público, mas também com o fornecedor. Afirma ainda que na questão de acesso a dados isso seria um problema, porque quando a empresa fornece informações para órgãos públicos, eles mesmos enquanto

fornecedores não têm mais acesso à informação e não se sabe se o órgão público que está armazenando a informação a está qualificando ou não. Nesse contexto, afirma que se houver qualquer problema com a informação, a empresa teria em teoria coparticipação.

Outra questão, para ele, é ter a base facilmente auditável; e essa auditoria deveria ser feita não somente por órgão governamental, mas também por órgão de controle público, da sociedade civil. Hoje, segundo José Guerrero, em nenhum lugar do mundo há órgãos independentes que façam auditoria desses dados, previstos tanto na legislação europeia quanto na brasileira. Isso é um problema que tem que ser resolvido, segundo ele.

José ainda faz uma provocação para os juristas, para que se pense quais as maneiras de compor leis ou composições sociais específicas para se ter acesso a dados que estão armazenados. Nesse contexto, menciona a questão de criptografia e acesso a dados criptografados. Hoje, na maioria das tecnologias de biometria facial, os dados seriam armazenados de forma não aberta, mas de forma facilmente detectável, e a partir desses dados armazenados, consegue-se recompor a face do indivíduo. Isso é um problema bastante sério, segundo ele, porque mesmo que o dado armazenado não seja um dado qualificado, com a engenharia reversa desse dado, consegue-se compor a imagem do indivíduo novamente.

Levando isso em consideração, José afirmou que enquanto fornecedor de tecnologia, elaborou uma tecnologia um pouco diferente, na qual não se usa pontos de face, referenciais de pele, cartilagem, dentro da montagem do modelo. Como consequência, uma vez que o modelo seja armazenado, mesmo que se faça engenharia reversa desse modelo, o que se monta é a estrutura craniana do indivíduo e não a estrutura da face dele, como numa foto. Ele afirma que essa cautela é bastante importante caso haja vazamento de informações.

PERGUNTAS DO PÚBLICO E RESPOSTAS DOS/AS PALESTRANTES

Não houve perguntas do público remoto, mas houve perguntas do público presencial, resumidas abaixo. O moderador pediu que preferencialmente fossem perguntas direcionadas a um membro específico da mesa. Nem todas conseguiram ser respondidas, em sua maioria por uma questão de tempo, pois o painel já estava se finalizando.

Após a rodada de perguntas da público, foi dada a palavra para cada palestrante. Abaixo, buscamos organizar as o conteúdo das palavras finais dos palestrantes às perguntas que interpretamos ser correspondente.

Paulo, do Instituto Beta, de Brasília - Achou importante lembrar o caso do episódio do antigo procurador geral da república, Rodrigo Janot. depois de uma declaração que não tinha a relação direta com dispositivos eletrônicos, foi expedido um mandado de busca e apreensão de dispositivo eletrônico por um ministro do STF.

Luan, pesquisador da FGV - Primeiramente, quis pontuar a questão do reconhecimento no tocante à população negra. Mencionou que esteve em um evento da Lavits esse ano e muitas pessoas negras falaram que preferiam não ser reconhecidas, porque esse não reconhecimento se tornaria uma forma de

proteção também. Queria ainda perguntar para Jacqueline ou Veridiana sobre a opção de uma moratória no banimento de uso do reconhecimento facial. É algo que está sendo discutido na literatura por alguns especialistas e até foi ventilado isso nos EUA e ele queria saber como se pensa essa aplicabilidade no Brasil.

Respostas:

José, sobre reconhecimento de negros e asiáticos, afirmou que caso se use um modelo de reconhecimento individualizado, consegue-se guardar informações segmentadas onde essa questão de a pessoa ser negra, asiática ou mulher passa despercebida, porque cada indivíduo é tratado como um modelo único; não há um modelo de massa, o aprendizado seria individualizado e teria como base características únicas de cada indivíduos.

Veridiana, sobre o banimento, afirma que EFF está nos EUA acompanhando de perto essas discussões. Até o momento, pela que ela teria conhecimento, essas discussões estão sendo realizadas em São Francisco, em Oakland e Somerville (Massachusetts). Aduz ainda que a EFF faz campanhas apoiando o banimento, via legislações locais, de reconhecimento facial em segurança pública. Em relação à América Latina, afirma que as organizações estão fazendo esse esforço de mapeamento, de entender onde está sendo utilizado, seja na segurança pública, seja nos serviços públicos, mas ela pessoalmente não tem conhecimento de legislações nesse sentido.

Milena Lima, delegada de polícia civil à disposição do Tribunal de Justiça - Perguntou a Jacqueline qual seria a atuação mais indicada no caso de uma situação de flagrante - por exemplo, num caso mais concreto, envolvendo pedofilia. Como poderia ter acesso ou não àquela informação? Afirmou, em sua pergunta, que no caso de flagrante haveria um tempo muito curto para poder avaliar, e às vezes a materialidade está no aparelho celular. Gostaria de saber qual a opinião de Jacqueline e também estende a pergunta para os demais da mesa que queiram comentar.

Respostas:

Jacqueline afirma que, pensando num procedimento mais adequado, que se realmente mesmo não for possível obter uma autorização judicial, se as informações essenciais para imputação de um crime de pornografia infantil ou outro a alguém serão perdidas, ela imagina que logo em seguida, com o relatório completo do que foi feito e no qual seja fundamentado o motivo que tornou necessário naquele momento já obter e coletar aquelas informações, articulando as informações sobre o porque não foi possível simplesmente apreender o dispositivo e levar para a delegacia ou levar diante de um juiz e pedir autorização para acessar. Ela imagina que nesse caso específico seria possível, mas ela pensa que seria necessário ter esse relatório. Ela alude que esse relatório seria submetido a um juiz que por sua vez iria verificar se realmente existiam as razões que justificariam esse acesso excepcional sem autorização judicial prévia. Mas esse caso seria muito excepcional, realmente a regra tem que ser mesmo a autorização judicial prévia. Aduz ainda que no crime citado realmente muitas vezes necessário acessar o dispositivo, caso diferente de uma agressão de um celular como objeto, em que realmente não seria necessário explorar o conteúdo do aparelho. Ela acredita que também com perícia se conseguiria recuperar o que se tem no celular e computador, então acredita que não haveria razão para atrasar essa autorização judicial e que o primeiro

pensamento deve ser mesmo correr para um juiz e pedir a autorização.

Dr. Rodrigo acredita que quase sempre será possível pedir um mandado não só de apreensão do celular, mas também para que seja acessado o conteúdo no celular nas limitações em que for necessário. Muito excepcionalmente, afirma que será possível utilizar o dispositivo do CPP relacionado à apreensão de coisas móveis, baseando-se nas fundadas razões da suspeita de que ali existiria prova de crime, apreendendo-se os bens e em seguida pedindo autorização para o juiz. Só seria necessário descobrir a senha, colocar em modo avião para o alvo nao apagar tudo à distância e tirar o chip para que não se conseguisse apagar parte dos dados.

Vagner Gama, gerente de informática do Cetam, de Manaus-AM - Fez perguntas a todos os membros da mesa. Para Dr. Rodrigo Prado, perguntou em relação aos crimes de caixa eletrônico,queria entender melhor porque não se consegue identificar as pessoas mesmo havendo câmeras. Pergunta também sobre a interceptação do WhatsApp. Para Veridiana Alimonti, pergunta sobre a autenticação de chave pública dizendo que queria entender melhor porque seria interessante que tenha nas duas pontas. Para Jacqueline, pergunta se ele for abordado por um policial que requeira o seu celular e eu ele não quiser entregar, como ele deveria proceder para guardar sua privacidade. Para José Guerrero, em referência a afirmação de que estamos em um “big Brother”, queria entender melhor se estamos sendo interceptados pelo próprio celular e também gostaria de entender a questão do armazenamento do fornecedor em bases próprias.

Nem todas as perguntas foram respondidas, por uma questão de compreensão e/ou tempo. As respostas recebidas às questões foram compiladas abaixo.

Dr. Rodrigo aduziu que hoje em dia a interceptação em dispositivos de criptografia de ponta a ponta é realmente inviável. A alternativa que existe é criar um “backdoor” para acesso que, se não for produzida no dispositivo, teria que ser inoculada no dispositivo através de um trojan, por exemplo. Existe também a possibilidade de utilizar a versão web no WhatsApp para espelhar o que está lá, mas quando a sessão deixar de ficar ativa, os dados seriam perdidos.

Veridiana responde que, na questão da autenticação, em primeiro lugar, nas comunicações de criptografia de ponta a ponta há a notificação da entrada de pessoas na conversa. No WhatsApp, há opção de ser notificado cada vez em que o código de segurança (security code) seja modificado e poderia ser checado o QR code ou a chave criptográfica de cada contato, para confirmar se a pessoa está enviando a mensagem para a pessoa certa.

José Guerrero respondeu que, quando se fornece tecnologia de algum cliente seja ele privado ou público, não há mais acesso ao controle da base de dados biométricos. Isso fica a controle do cliente. Assim, é garantido que a base não será mais compartilhada com nenhuma outra empresa, e não se tem mais acesso aos dados, que podem ser vazados ou não. E, se acontecer algum problema com aquele órgão específico, a empresa será arrolada junto ao processo por ser fornecedora da tecnologia.

QUADRO COMPARATIVO

Diante das inúmeras discussões trazidas no debate, destaca-se os tópicos abaixo. É importante pensar, no entanto, que os pontos não foram abordados

por todos os membros da mesa e, nesse sentido, não se pretende uniformizar os posicionamentos, mas sim realizar um exercício de síntese dos pontos elencados a seguir.

TIPO DE MANIFESTAÇÃO (POSICIONAMENTO OU PROPOSTA)	CONTEÚDO	CONSENSO OU DISSENSO	PONTOS A APROFUNDAR
Posicionamento	Parâmetros e limites à atuação estatal na utilização das TICs no âmbito da segurança pública.	Necessidade de haver parâmetros para que utilização das TICs pelo não se dê de forma abusiva e em desrespeito a garantias fundamentais. Apontou-se questões como a previsão legislativa e a necessidade de autorização judicial para determinados casos. Também mencionou-se a participação da sociedade civil nessa fiscalização.	
Posicionamento	Lei, jurisprudência e mudanças e inovações tecnológicas	O aparato jurídico (em especial a legislação e a jurisprudência) não acompanham a rapidez do desenvolvimento e de inovações tecnológicas. Isso traz consequências para a persecução criminal. Ventilou-se consequências diversas disso como: comprometimento das atividades estatais na persecução penal, aumento da repressão, e dificuldade de controle da	

		sociedade civil nesse sentido. As visões são, portanto, variadas.	
Posicionamento	Mecanismos discriminatórios de grupos socialmente vulneráveis	Diversas razões levam a que esses mecanismos ganhem caráter discriminatório quando aplicados, em especial no que concerne a grupos social e estruturalmente vulneráveis como mulheres e a população negra. Reconhece-se um maior número de falsos positivos gerados contra esses grupos.	
Posicionamento	Exigência de decisão judicial prévia para a utilização das TICs na persecução criminal.		Ainda que seja muito importante a exigência do requisito formal (decisão judicial), um ponto a aprofundar é a questão de requisitos não só formais, como a citada decisão fornecida por um juiz, mas também requisitos efetivamente materiais, fáticos, que devem ser observados quando na utilização das TICs na persecução criminal.
Proposta	Apreensão de dispositivos móveis pela polícia		Proposta de aprofundamento sobre como lidar e responder à casos em relações aos quais se têm relato, nas quais a polícia

			pede e por vezes tenta apreender dispositivos móveis em abordagens rotineiras, em que não estão presentes os requisitos legais de busca e apreensão?
Proposta	Auditoria dos bancos de dados de informações de biometria facial.		Pensar em como se daria essa fiscalização/controle desses bancos de dados.