DIÁLOGO

"NECESSITAMOS DE MAIS TRANSPARÊNCIA E DEBATE SOBRE O USO DE TECNOLOGIAS DE VIGILÂNCIA"

• *Entrevista com Jamila Venturini e Michel Roberto de Souza - Derechos Digitales* •

Por *Revista Sur*

A Derechos Digitales[1] é uma organização de alcance latino-americano, comprometida com a defesa e a promoção de direitos humanos no entorno digital, que trabalha em três frentes principais: Liberdade de expressão, Privacidade e Direitos autorais e acesso ao conhecimento.

Para esta edição, a equipe da Revista Sur *teve a oportunidade de conversar com Jamila Venturini, codiretora executiva, e Michel Roberto de Souza, diretor de políticas públicas da organização. Nosso interesse principal, além de conhecer os resultados da pesquisa recentemente publicada pela Derechos Digitales sobre casos de reconhecimento facial na América Latina[2] era escutar, a partir de informações de uma organização especializada no tema e com foco na região, as razões do crescimento acelerado do uso de tecnologias de vigilância e reconhecimento facial e os riscos resultantes para os direitos humanos.*

Questões abordadas nesse diálogo incluem, por exemplo, as legislações local e internacional; relações econômicas e políticas entre fabricantes, provedores e compradores; detalhes da aplicação dessas tecnologias em diferentes contextos no continente; o impacto da pandemia de Covid-19 na legitimação de maior vigilância aplicada ao controle do espaço público e privado; o aprofundamento da discriminação racial e migratória; assim como os principais desafios para a região em termos de garantia de direito à privacidade, autonomia e acesso à informação da cidadania.

Revista Sur • Nos últimos anos temos observado um panorama de avanço das tecnologias de vigilância em países do Sul Global. Qual análise vocês fazem desse cenário?

Jamila Venturini • Nossas preocupações com vigilância e privacidade no contexto digital estão muito ligadas a uma constatação de que as tecnologias se somam a um histórico de abusos contra os direitos humanos e criminalização de grupos que se contrapõem às estruturas de poder estabelecidas na América Latina. Elas podem, por um lado, facilitar a intrusão em comunicações privadas e, por outro, permitir o acesso a informações que até então não estavam disponíveis para autoridades policiais ou governos autoritários. Um exemplo são os metadados, ou seja, os "rastros" que deixamos a cada interação com dispositivos digitais. Eles incluem geolocalização, horários e duração da conexão à internet ou acesso a determinada página ou plataforma etc., e são capazes de revelar hábitos individuais íntimos e sensíveis sobre onde e com quem vivemos, nossa rede de contatos, interesses e pensamentos, nossos períodos de sono... Infelizmente, há uma série de exemplos de abusos em relação ao uso desse tipo de informação, por parte do setor público ou por empresas.

Junto a uma série de desenvolvimentos legislativos que buscam facilitar o acesso governamental a informações privadas coletadas por empresas provedoras dos mais variados tipos de tecnologias, observamos o crescente interesse regional pela compra de sistemas de vigilância. Além de registrar o que ocorre em espaços públicos ou semipúblicos, eles buscam extrair ainda mais informação de comportamentos humanos ou forçar o acesso a dispositivos, como é o caso dos sistemas biométricos – como os de reconhecimento facial – e *softwares* maliciosos, também conhecidos por *malware*.

Esse interesse advém em grande medida de uma percepção de que as tecnologias vão ajudar a solucionar problemas sociais. No âmbito da segurança pública, essa retórica defende tanto a compra das mais variadas tecnologias, como reformas no âmbito normativo que permitam sua utilização. Cabe ressaltar que a América Latina é uma região mormente consumidora de tecnologias estrangeiras e não se destaca pela produção local. Nesse sentido, há uma grande preocupação sobre como os países latino-americanos se tornam um mercado privilegiado para as fabricantes e distribuidoras de tecnologias de vigilância, especialmente quando os controles se incrementam em outras regiões do mundo.

Sur • Como tem se desenvolvido o debate sobre o vigilantismo a partir do cenário brasileiro?

JV • No Brasil sabemos o quanto esse tipo de tecnologia avança nas pequenas cidades, em espaços públicos diversos de maneira rápida e com pouquíssima transparência. A forma como a cidadania fica sabendo que essas coisas estão acontecendo é quando elas chegam à imprensa ou quando se identifica uma compra pública de câmeras, por exemplo, por meio de um processo de licitação. Em todos os casos, quando já é tarde demais e a compra ou adoção dessas tecnologias já está avançada. Isso num país que tem um histórico de autoritarismo e abusos. Não necessariamente os avanços legislativos e normativos existentes dão conta das garantias necessárias para poder usar esse tipo de tecnologia de maneira alinhada com os

compromissos de direitos humanos assumidos pelo Brasil. Não é um debate simples, e são necessários critérios muito específicos sobre como tecnologias de vigilância serão utilizadas e os limites para essa utilização.

Michel Roberto de Souza • É relevante também mencionar a imprensa e os jornalistas, que têm um histórico de censura e perseguição na região. Temos visto muitos exemplos em que a patrulha do Estado começa no digital, o que chamamos *ciberpatrullaje*,[3] com coleta de informações de várias fontes, inclusive abertas, na internet, cuja motivação e fins são, na maioria dos casos, questionáveis, pois contribuem para estigmatizar jornalistas, ativistas e defensores dos direitos humanos com opiniões distintas do governo que está na gestão atual. Utiliza-se de buscas nas redes sociais, com acesso ao telefone e aplicativos de espionagem, como no recente caso do Pegasus. Fica muito claro que essa violação de direitos começa no [ambiente] digital, mas isso vai parar no físico. E as tecnologias acabam aumentando as possibilidades de perseguição. Por isso é importante a questão dos rastros deixados na internet, da necessidade de criptografia de ponta a ponta, entre outras questões para a proteção dos direitos humanos.

No caso do reconhecimento facial em locais públicos, isso é elevado à enésima categoria. Com essa tecnologia é possível saber quem é aquela pessoa, as características do movimento dela, saber com quem ela está falando. São várias informações, e muitas delas extremamente sensíveis, mesmo em espaços públicos, que são coletadas por câmeras muitas vezes escondidas. Isso sem falar nos graves problemas relacionados à discriminação e falsos positivos, além da possibilidade de cruzamento dos dados do cidadão com outras e diversas bases de dados.

Vemos esta tendência na América Latina inteira, do Estado querer ter mais dados dos cidadãos. Criam-se bancos de dados gigantescos, e com o reconhecimento facial simplesmente esses dados são tomados e cruzados com os dados da rua, dos metrôs, do dia a dia, o que gera uma quantidade enorme de informações sobre todo mundo. Mas quem é todo mundo? É jornalista, é ativista de direitos humanos, é quem vai fazer protesto na rua, mulheres, pessoas transexuais, crianças e adolescentes, migrantes, enfim... Os riscos são muitos, podendo ter ameaças à reunião pacífica, ao próprio direito de protesto – é possível saber quem está protestando, pois é muito fácil saber e fazer esse cruzamento –, ameaças à liberdade de movimento e circulação também, à presunção de inocência, de não ser considerado culpado e não ser investigado sem um devido processo legal. Esse uso da tecnologia levanta questionamentos muito graves também sobre privacidade, intimidade e proteção de dados.

***Sur* •** De que forma ocorre essa exposição de dados e informações e qual a sua relação com práticas discriminatórias?

MRS • Esses dados que são coletados num sistema de reconhecimento facial são dados biométricos sensíveis e armazenados em algum lugar. Mas é preciso questionar, como se dá esse armazenamento? Quem tem acesso? Quais dados são cruzados? Quais bases de dados

podem ser utilizadas? Pode ter algum risco com relação à segurança? Vimos recentemente uma organização do México, a R3D, que reportou um caso de grave vulnerabilidade dessas câmeras de segurança, com a possibilidade de que sejam invadidas de uma forma muito fácil.[4] Então temos um Estado que é supervigilantista, mas essa própria vigilância tem falhas gigantescas de segurança que expõem ainda mais o cidadão, sem contar os questionamentos sobre a legalidade desse supervigilantismo.

Há graves riscos à liberdade de expressão, de censura, com um efeito perceptível pelo esfriamento do debate público e a autocensura, porque a pessoa sabe que ela está sendo vigiada. Isso é muito claro com relação a jornalistas e pessoas defensoras de direitos humanos. Há a dificuldade, por exemplo, de fazer investigações, de manter contatos com fontes de informação, porque tudo vai estar nesse ambiente de vigilância. Fora as questões de discriminação, que estão ocorrendo no mundo de forma muito incisiva por conta principalmente das falhas dessas tecnologias para lidar com pessoas que não são homens brancos. Ou seja, basicamente para lidar com mulheres, para lidar com pessoas de pele escura, com pessoas negras e com crianças também. Há vários problemas relacionados à discriminação, com prisões arbitrárias e outras ilegalidades. E questões de migração, pois sabemos que cada vez mais os imigrantes estão sendo vigiados de várias formas, que os Estados têm se utilizado das mais variadas tecnologias com fins de vigilância.

Temos discutido muito como a tecnologia tem sido utilizada para deslocar as pessoas migrantes, inclusive com casos graves de acesso aos telefones celulares e redes sociais, entre outros abusos. E os casos não ficam restritos às regiões de fronteira, mas igualmente envolvem casos de reconhecimento facial nas cidades para saber onde estão os migrantes, com quem eles estão falando, se estão em uma situação legal no país ou não.

Assim, há altos riscos relacionados à tecnologia em um sentido mais lato, mas também ao reconhecimento facial num sentido mais estrito. A utilização de ferramentas com a chamada inteligência artificial vem sendo muito debatido em termos de utilização de tecnologia, e de tecnosolucionismo, no sentido de que a IA poderia ser usada e pode ser boa para tudo, desde a tarefa mais simples até a mais complicada. O reconhecimento facial também se utiliza de uma inteligência artificial, por isso as coisas se conectam.

Sur • Pensando na América Latina, quais seriam as contradições identificáveis em relação à valorização das ferramentas tecnológicas de vigilância e o cerceamento de liberdades individuais e coletivas, por exemplo?

JV • São muitas contradições que observamos em nossa região, que é muito diversa inclusive em relação a como se usam essas tecnologias de vigilância. Um primeiro ponto a destacar é que a vigilância persiste em seu caráter mais arcaico, com agentes perseguindo opositores políticos em determinados países, e chega a elevados níveis de refinamento, com a instalação de antenas de captura de comunicações, câmeras de reconhecimento facial ou a instalação de *software* malicioso. Esse tipo de estratégia tem sido utilizado

contra jornalistas, movimentos sociais e pessoas defensoras de direitos humanos com o objetivo de silenciar, criminalizar e de perseguir esses grupos.

Um segundo ponto está relacionado à pergunta, que já é quase um clichê, "quem vigia o vigilante?". Por um lado, observamos uma tendência crescente na coleta de dados da cidadania por parte dos Estados; por outro, há uma tentativa de fechar cada vez mais as possibilidades de acesso à informação pública e várias limitações em relação às iniciativas de transparência pública. Isso ficou evidente durante a pandemia: enquanto os governos lançavam suas estratégias baseadas na coleta de dados sensíveis sobre fluxos de movimentos e condições de saúde, eles buscavam ao mesmo tempo restringir o acesso à informação da cidadania sobre as ações do próprio Estado. Isso foi super evidente no caso brasileiro e é totalmente inaceitável. Qualquer ação estatal que possa resultar em uma limitação ao exercício de direitos fundamentais deve ser acompanhada, entre outras, de estritas medidas de transparência, como apontam vários órgãos e autoridades internacionais de direitos humanos.

Finalmente, é importante reconhecer que a vigilância também ocorre de maneira desigual nas sociedades e está dirigida de maneira diferenciada a determinados grupos. Quando se propõe instalar câmeras de reconhecimento facial no metrô, por exemplo, ou em qualquer meio de transporte público, isso atinge as pessoas que usam o transporte público, e não aquelas que contam com outras opções. Essa discussão não é nova, mas é sempre importante enfatizá-la. A vigilância afetou e afeta as populações que historicamente foram mais marginalizadas e, com o auxílio de novas tecnologias como a inteligência artificial, ela pode reforçar desigualdades. Já vemos na região como certas tecnologias são utilizadas para legitimar intervenções estatais em contextos de grande vulnerabilidade. Na Argentina e no Chile, por exemplo, já se busca utilizar sistemas para "prever" situações como gravidez na adolescência, evasão escolar, entre outras, a partir da coleta e cruzamento de uma série de informações pessoais. Em outros países, propostas de uso de policiamento preditivo – extremamente questionadas no âmbito internacional – estão sendo testadas.

Sur • Qual é a percepção de vocês em relação à normatividade e sua capacidade real de limitar a ação perversa das tecnologias de vigilância?

JV • Os cenários variam a depender do país e da tecnologia em questão. Uma coisa é falar sobre interceptação telefônica e telemática,[5] e há uma série de critérios muito estritos que deveriam ser seguidos em termos de procedimento para que ocorram da forma menos intrusiva possível e em casos muito específicos e limitados. Nesse sentido existe maior consenso e regras estabelecidas que poderiam ser extrapoladas para outras práticas, como a *ciberpatrullaje*, a quebra de criptografia, entre outras. A videovigilância e o reconhecimento facial, por sua vez, são formas de vigilância em massa, e existem muitos questionamentos sobre até que ponto são compatíveis com o marco de direitos humanos existente que está fundamentado em critérios de legalidade, necessidade e proporcionalidade.[6]

Existe um amplo debate internacional sobre a legitimidade da compra e venda de tecnologias de vigilância e a necessidade de uma moratória ou proibição desse tipo de negócio, tanto devido à fragilidade institucional dos países compradores, como por conta da falha das empresas produtoras de garantir que elas não geram riscos aos direitos humanos. Sobre essas empresas recai a responsabilidade de garantir que as tecnologias que produzem são seguras, não geram riscos excessivos aos direitos humanos e não são oferecidas a governos autoritários.

No entanto, dado o avanço dessas tecnologias de forma indiscriminada na região, inclusive na ausência de normas específicas, é necessário pensar em quais as regras necessárias para dar conta de mitigar riscos, assim como para garantir que haja instâncias de revisão e de supervisão com participação democrática.

MRS • Como, onde e com quais ferramentas regulamentar são questões que ainda estão em aberto, porém temos algumas pistas. A Michelle Bachelet, Alta Comissária de Direitos Humanos da ONU, publicou nos últimos meses um relatório muito preciso e importante que apontava para os altos riscos do uso de tecnologias e de inteligência artificial para a sociedade e pediu a moratória da utilização desse tipo de tecnologia até que os Estados consigam cumprir uma série de requisitos de respeito aos direitos humanos,[7] considerando-se o desenho da vida dessa tecnologia, do começo ao fim. Esse acompanhamento é extremamente necessário.

Sur • Quais são os principais desafios, em termos de direitos humanos, privacidade e segurança, que o reconhecimento facial como estratégia de vigilância e controle impõe para as organizações de direitos humanos na América Latina?

MRS • Muitas vezes temos dificuldade em entender como funcionam as tecnologias e como têm sido aplicadas, pois estamos falando de contextos de extrema opacidade. Não se sabe quem faz, como faz, qual é a lei que as legitima. Elas também não têm uma finalidade específica, em contextos em que não há nenhuma participação social. Parece uma questão meramente administrativa, do dia a dia, e por isso se entende que não seria preciso ouvir a população, não seria preciso ouvir as pessoas que vão ser impactadas, que o próprio debate sobre o impacto não seria necessário. Mas é justamente o contrário: necessitamos de mais transparência e debate sobre o uso de tecnologias de vigilância em face dos enormes impactos negativos nas vidas das pessoas. Diante dessa opacidade, por exemplo, no tema do reconhecimento facial, a Derechos Digitales publicou e mantém um site[8] e recentemente fez uma pesquisa junto com o consórcio Al Sur, que reúne 11 organizações da América Latina, e identificamos cerca de 40 iniciativas de uso de reconhecimento facial na região. No Brasil, foram identificadas 4 ou 5 iniciativas, mas sabemos que existem muito mais.[9] Então a própria existência desse tipo de tecnologia vigilantista já é um enorme desafio.

Estudos mais recentes de outras organizações demonstram desafios que são gigantescos na adoção de tecnologias sem o devido cuidado em respeitar os direitos humanos. No Brasil, organizações estão olhando como o reconhecimento facial interfere em direitos de

pessoas trans, por exemplo. A Coding Rights fez esse estudo, e são pesquisas extremamente importantes porque estão dando outra perspectiva para os problemas e impactos negativos da utilização dessa tecnologia.[10]

É importante questionar, dar mais transparência. Mas quando fazemos perguntas para o poder público, ele simplesmente não tem resposta, apenas uma ideia de que vai solucionar alguma coisa, resolver algum ou vários problemas de uma vez só, que isso vai ser bom para a segurança pública, que vai diminuir a criminalidade, mas não sabe como de fato essa tecnologia vai solucionar o problema. Nos fóruns internacionais, a própria ONU recentemente revisou a resolução sobre privacidade na era digital, trazendo os riscos do uso de tecnologias biométricas e de inteligência artificial. Do mesmo modo, a UNESCO aprovou um acordo sobre inteligência artificial tentando levantar algumas questões, inclusive enfatizando a necessidade de utilização de avaliação de impacto ético (*ethical impact assessment*).[11]

Sur • Como funciona a conscientização voltada aos públicos diretamente afetados e como têm sido pensadas as estratégias e esse diálogo da própria sociedade civil organizada?

JV • Como comentei antes, geralmente a sociedade civil fica sabendo dessas tecnologias quando já é tarde demais, ou seja, quando o processo de compra já está em andamento. Então, uma alternativa de ação envolve o questionamento judicial buscando barrar a implementação e obter informação.

Há uma série de casos que observamos, nesse levantamento que foi feito, por exemplo, em que há uma gestão administrativa muito precária. Então, o fato de termos essa limitação em como se apresenta a discussão dentro de um marco de direitos humanos reflete um pouco essas dificuldades que temos mencionado. E não necessariamente isso é exclusividade das tecnologias de vigilância ou dos sistemas de reconhecimento facial, pois estamos num momento de retrocesso muito grande em relação à agenda de direitos humanos na região. Mas, sim, ainda há muito por se fazer em relação a como entendemos esses critérios de legalidade, necessidade, proporcionalidade quando se trata de sistemas de reconhecimento facial e de tecnologias de vigilância.

Existe um desafio nesse sentido, mas, ao mesmo tempo, o grande esforço de conscientização precisa, nesse momento e enquanto essas tecnologias avançam dessa forma tão intensa, estar colocado nas pessoas que fazem a gestão pública, em quem está lidando com as contratações, quem está lidando com as decisões, nos formuladores de políticas públicas e no Poder Judiciário para fazer o controle efetivo de como elas são implementadas. Porque estamos falando de algo que escapa ao debate legislativo.

O debate chega depois do avanço administrativo dessas tecnologias e, muitas vezes, inclusive, após o seu questionamento judicial. Enquanto sociedade civil, também é importante entender essas tendências e tentar mapear o que está acontecendo, onde elas são implementadas, quais são as empresas que estão tentando empurrar isso, porque aí é possível também

encontrar outras estratégias, outras formas de reagir, inclusive fora da região, por exemplo, nos países de origem dessas empresas, em outros tipos de fórum. Ainda existem desafios, e uma preocupação urgente é como nos apropriamos desse debate enquanto organizações de direitos humanos, como reagimos a essas iniciativas, que tipo de argumentos vamos trazer... Existe muito desconhecimento, e a gente observa, lamentavelmente, tentativas de utilizar ou apoiar tecnologias desse tipo advindas até de organizações da sociedade civil. Precisamos continuar trabalhando em conjunto para ter uma compreensão comum e, no seguinte passo, junto a formuladores e formuladoras de políticas públicas. Com certeza, conquistar a opinião pública é um objetivo, mas o desafio é muito maior também em relação a como nos mobilizamos socialmente em favor dos direitos humanos de maneira mais ampla.

MRS • O debate está saindo um pouco do nicho de quem lida com tecnologia. As preocupações têm ido cada vez mais para a sociedade civil de uma forma ampla e a quem está lidando com os temas diariamente. Por exemplo, para quem está lidando com os temas de racismo, direitos de crianças e adolescentes, migração, liberdade de imprensa e com outros temas. Está se criando um caldo da sociedade civil com relação ao tema do reconhecimento facial em específico, mas também com relação à utilização de outras tecnologias para fins de vigilância. Mas falta ainda uma percepção de que isso de fato é um risco e um problema de direitos humanos. E esse é o primeiro momento, identificar isso como um problema nas mais diversas áreas de atuação da sociedade civil, para depois conseguir influenciar e tentar fazer litígios estratégicos que tenham mais participação de vários atores.

A participação social precisa ser fomentada nas mais diversas áreas. Eu, enquanto advogado que lida com tecnologia, direitos humanos e litígio, vejo uma questão de tecnologia de determinada forma. Agora, quando um jornalista, ou uma associação de jornalistas, está lidando com uma questão de tecnologia, ela está vendo de outra forma. Há uma riqueza imensa nessa troca de conhecimento. Em alguns países a percepção do uso dessas tecnologias como um problema é muito evidente, como no México, com todos os ataques que estão acontecendo por lá e a importância de se verificar como a tecnologia tem sido utilizada para violar direitos. Isso vai expondo e criando possibilidades de defesa por parte da sociedade civil diante de um momento de ataque, como uma necessária resistência.

Sur • A partir da pesquisa que desenvolveram, como vocês enxergam a relação entre os países que estão produzindo essas tecnologias e os países da América Latina, e como acontece esse *lobby*, principalmente na questão de segurança pública, que é uma das áreas em que talvez elas estejam sendo mais utilizadas?

JV • O que fizemos foi um mapeamento. Identificamos, por exemplo, que há empresas internacionais atuando na região de diferentes formas. Há muitos anos – pelo nosso mapeamento desde os anos 1990 – existem acordos de vários países com essas empresas. E geralmente também há revendedoras locais desses sistemas internacionais. Outra situação que observamos, e já era uma hipótese nossa, envolve empresas chinesas. Tem outra forma de atuação em que elas oferecem os serviços e, ao mesmo tempo, o Estado chinês oferece o financiamento para

a contratação daqueles serviços. É quase como se fosse uma doação do serviço. Também há a situação em que aquilo não tem custo econômico ou tem um custo reduzido.

E aí quando pensamos em reconhecimento facial, há várias provedoras que se envolvem, desde aquelas de infraestrutura, de telecomunicações etc. Desde empresas nacionais até internacionais. É interessante observar como as empresas internacionais estão operando com apoios e contratos milionários na região, no caso mais evidente, as empresas chinesas proibidas de operar em alguns países com suspeitas graves de envolvimento ou de utilização dos seus sistemas em contextos de violação de direitos humanos. No México, especificamente, encontramos esses casos. Por outro lado, o fato de que seja uma cadeia tão complexa torna ainda mais difícil identificar todos esses agentes e as capacidades de cada um.

Desta maneira, quando pensamos em *lobby* e como as empresas atuam aqui, uma questão é: parece existir uma diferença entre como elas operam nos seus países de origem e como elas operam na região, não necessariamente em relação a reconhecimento facial. No ano passado, várias empresas declararam que não venderiam suas tecnologias de reconhecimento facial para polícias. Mas quando se tenta entender mais sobre essa declaração, às vezes, ela está limitada a um escopo nacional. Por exemplo, nos Estados Unidos, no contexto do [movimento] Black Lives Matter, várias empresas, como a Amazon, a IBM, a Microsoft, entre outras, declararam que não iam vender sistemas, mas não ficava tão evidente se eles não seriam vendidos globalmente, se eles não seriam vendidos somente lá, para quem não seriam vendidos, por quanto tempo... São as limitações desse tipo de medida proativa. Então um grande desafio é entender como essas empresas se veem globalmente. Outro desafio, quando se trata de empresas de vigilância, tem a ver com até que ponto existem mecanismos de solicitação de prestação de contas por parte dessas empresas e até que ponto têm sido efetivas essas medidas. A gente consegue ter um pouco essa dimensão, sem tanta evidência de um *lobby*, mas sabemos que muitas vezes são relações diretas que acontecem no âmbito administrativo entre vendedores e compradores.

A Derechos Digitales é membro de uma organização global chamada Global Network Initiative (GNI), composta por várias partes interessadas (*multistakeholder*) e que reúne empresas, organizações da sociedade civil e a academia que tratam de resistir a obrigações impostas por Estados específicos e que são abusivas em relação à privacidade e liberdade de expressão. Essas coisas vão variar muito em relação ao que se está discutindo normativamente, qual é o setor da empresa e certamente também em relação ao país. Quando se trata de reconhecimento facial de modo específico, como não existe uma discussão legislativa tão forte, as formas de influência vêm de outros lados.

MRS • Algumas empresas já declararam que não vão utilizar essas tecnologias e que se autoimpuseram, digamos assim, uma moratória com relação ao reconhecimento facial. Mas, ao mesmo tempo, elas querem uma regulamentação. O discurso é de que seria necessário regulamentar de alguma forma para evitar riscos maiores aos direitos humanos. A verdade é que isso é um grande mercado, mundial e bilionário, da segurança pública, mas também o

mercado do reconhecimento facial e do vigilantismo em geral. Sabemos que tem muita empresa fazendo *lobby* legislativo, mas há uma dificuldade em saber quem são, quais são os interesses e os argumentos que estão sendo levantados. Esta dificuldade aumenta quando pensamos num contexto mais local, por exemplo, em escolas e em projetos de cidades inteligentes. Saber de fato quem está fazendo *lobby* é difícil. Temos alguns indícios, algumas suposições…

Sur • Quais são as perspectivas futuras para esse debate?

JV • Há alguns anos imaginávamos que poderíamos estar, nesse momento atual, com uma agenda positiva e propositiva em relação ao uso de tecnologias. Essa agenda existe e persiste, ela continua estando no centro das nossas preocupações. Mas estamos vivendo um momento de muitos desafios, de muito retrocesso, que pode ser agravado por essas tecnologias de vigilância, o que faz com que a gente tenha que se mobilizar cada vez mais para resistir em relação a elas e para tentar conscientizar sobre os riscos que elas trazem. Às vezes, podemos nos sentir um pouco tecnofóbicos, para pegar o extremo oposto do tecnosolucionismo, mas boa parte dos esforços que precisam ser feitos nesse momento, em que muitas dessas tecnologias têm um apelo grande na sociedade, em diferentes setores, nos Estados etc., é tentar desnaturalizar alguns pressupostos por trás do uso dessas tecnologias. Considero que é fundamental uma visão crítica para estabelecer as bases para o diálogo sobre o que queremos do uso das tecnologias, o que queremos das normas que vão regular usos que eventualmente sejam necessários, que sejam específicos, inclusive no âmbito de investigações. Como eu disse no início, existem situações em que será necessário eventualmente recorrer a determinadas tecnologias e determinadas informações, mas isso precisa estar muito limitado. Infelizmente, o que percebemos como tendência é o contrário, é uma tentativa de liberalizar ao máximo esses usos e esse acesso.

Com isso, estamos neste momento de defesa dos nossos direitos mais fundamentais, sabendo que, quando se fala em privacidade, falamos de um direito que é instrumental para vários outros direitos. Então é importante entender isso: não se trata simplesmente de um direito individual, do meu direito a não ser incomodada nas minhas comunicações; se trata basicamente da minha possibilidade de interagir e me desenvolver com autonomia, de me expressar com liberdade. E com isso também permitir que a sociedade como um todo possa ter acesso a uma série de outras informações, e de visões sobre futuro, sobre a realidade. As coisas estão muito interconectadas, estamos falando de coisas que também afetam o quanto a nossa democracia pode florescer ou não, e não só de questões individuais. E é fundamental trazer isso de volta para a conversa.

• • •

Entrevista conduzida pela equipe da Revista Sur *em novembro de 2021.*
Original em português.