Vigilância biométrica remota na América Latina

As empresas estão respeitando os direitos humanos?

O que pedimos às empresas

Em Agosto de 2021, a Access Now, Asociación por los Derechos Civiles (ADC, Argentina), Laboratório de Políticas Públicas e Internet (LAPIN, Brasil), e LaLibre.net (Equador), lançaram o relatório, "Tecnologia de Vigilância na América Latina – Feita no Exterior, Implantada em Casa", destacando a venda e utilização de tecnologias de vigilância biométrica remota na região. Antes da publicação, demos a todas às empresas envolvidas uma oportunidade de compartilhar suas contribuições - nenhuma optou por fazê-lo.

Em 2022, a Access Now ampliou seu trabalho sobre o assunto, lançando a campanha #PorQuéNosVigilan (por que nos vigiam) sobre os perigos da tecnologia de vigilância em massa implantada em países de América Latina. A Access Now também fez uma parceria com o Business and Human Rights Resource Centre para obter respostas das empresas que implantam tecnologia com capacidades de vigilância na região. Como resultado, nove das 23 empresas que tínhamos mencionado em nosso relatório de 2021 reagiram, enquanto as demais 14 permaneceram em silêncio.

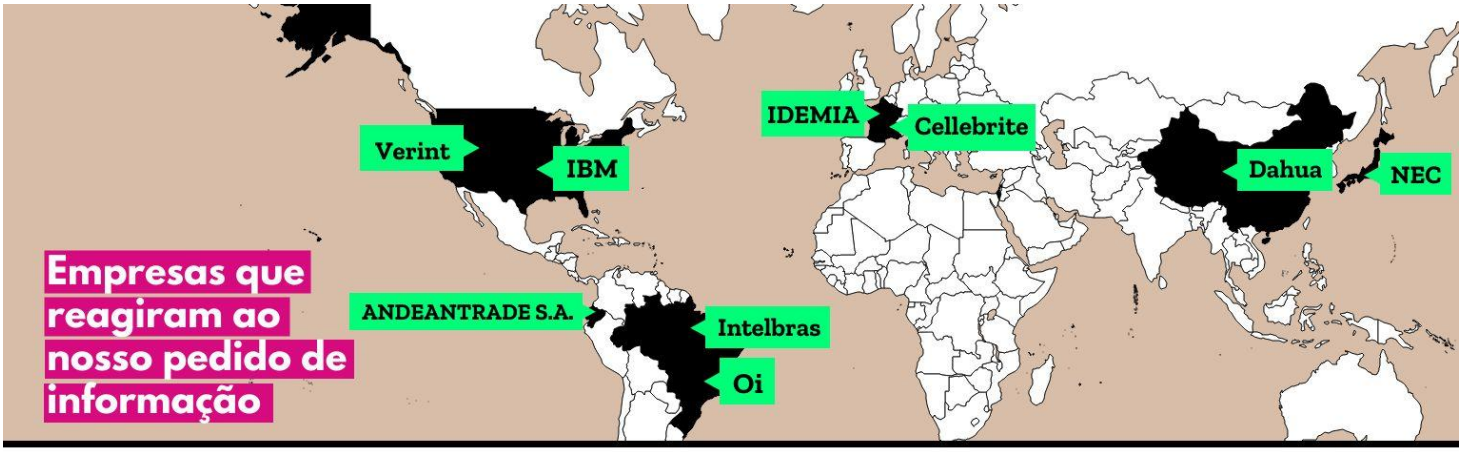
As limitadas reações que recebemos fizeram pouco para esclarecer o escopo da tecnologia com recursos de vigilância implantados na região; a maioria das empresas forneceu apenas

uma resposta geral, em vez de responder a cada uma de nossas perguntas específicas. Também observamos que algumas respostas sugerem que as empresas não estão em conformidade com os United Nations Guiding Principles on Business and Human Rights [Princípios Orientadores sobre Empresas e Direitos Humanos da Organização das Nações Unidas] (UNGPs), principalmente quando se trata de compromissos de respeito aos direitos humanos, de realizar a devida diligência para identificar e prevenir violações salientes aos direitos humanos, e de fornecer abertamente informações sobre como as empresas estão cumprindo com as leis aplicáveis.

As empresas devem se comunicar de maneira aberta e transparente com o público sobre as medidas tomadas para abordar o impacto que suas atividades podem ter sobre os direitos humanos, especialmente quando as preocupações são levantadas, direta ou indiretamente, por comunidades ou indivíduos afetados. Ficar em silêncio sobre essas questões é uma forma de evitar a responsabilização e dificultar a avaliação de suas atividades por especialistas independentes.

O documento a seguir analisa as respostas que recebemos e até que ponto as informações fornecidas se alinham com os UNGPs.

Empresas que responderam à nossa solicitação de informações



- **ANDEANTRADE S.A**
- BGH Tech Partner
- **Cellebrite**
- **Dahua**
- Danaide
- El Corte Inglés
- Full Tecnología FullTec CIA. LTDA
- Hikvision
- Huawei
- IAFIS Argentina S.A
- **IBM**
- **Idemia (former Morpho)**
- **Intelbras**
- Johnson Controls
- **NEC**
- **Oi**
- Oosto (former Anyvision)
- RC International
- Security Team Network S.A
- Unión Eléctrica S.A.
- Unitech S.A
- **Verint***
- ZTE

Empresas que responderam.
Empresas que não responderam.

*** A resposta da Verint informou apenas que seu "negócio de segurança cibernética agora é uma empresa pública independente chamada Cognite Software Ltda." Entramos em contato com Cognyte, que originalmente estava aberta para conversar, mas eles nunca confirmaram uma data.**

Os problemas de base das respostas das empresas

Nas respostas que recebemos, identificamos diversos padrões recorrentes:

1. Esquivar-se da responsabilidade ao descaracterizar seus produtos

A **Cellebrite** se opôs à caracterização de seus produtos como ferramentas de vigilância, descrevendo-os como "soluções de inteligência digital" usadas em investigações no cumprimento da lei. Ao deixar de reconhecer que a vigilância é um risco evidente aos direitos humanos em seus serviços ofertados, essas empresas não podem realizar a devida diligência para identificar e prevenir o impacto aos direitos humanos, conforme exigido pelos UNGPs.

Enquanto isso, a **IDEMIA** (antiga Morpho) negou ter "qualquer tipo de tecnologia de vigilância na Argentina, Brasil ou Equador". Eles disseram que seus sistemas usados "nestes países são para utilização de identificação biométrica para prática forense" – uma afirmação desmentida em informações compartilhadas pelas autoridades.

Na realidade, as agências policiais argentinas começaram a usar os produtos Morpho antes de 2010, e a IDEMIA é responsável por instalar e estabelecer o Sistema Automatizado de Identificação de Impressões Digitais (AFIS) do Ministério da Segurança. Atualmente, tecnologia da IDEMIA está em uso em toda a Argentina, como nas cidades de Campana, Luján, Balcarce, Córdoba, Chaco e várias cidades da Província de Buenos Aires.

Acima de tudo, a resposta da IDEMIA ignora a realidade de que a tecnologia que permite o reconhecimento biométrico remoto *é* tecnologia de vigilância e pode causar ou contribuir para impactos negativos sobre os direitos humanos. A empresa optou por contestar fatos específicos e interpretou erroneamente nossas constatações, como ao tentar esclarecer que a Morpho RapID usa impressões digitais, quando nosso relatório diz o mesmo, e são dados biométricos.

Em suas curtas respostas, nem a Cellebrite nem a IDEMIA mencionaram os direitos humanos, muito menos sua responsabilidade corporativa de respeitar esses direitos. Isso viola diretamente o Princípio 11 dos UNGPs: "As empresas devem respeitar os direitos humanos. Isso significa que elas devem se abster de violar os direitos humanos e devem abordar os impactos adversos nos direitos humanos com os quais tenham envolvimento."

2. Desviar sua responsabilidade para outros atores

Diversas das empresas tentaram se distanciar das ações de seus parceiros. A **Andeantrade**, uma fornecedora de produtos Hikvision, concentrou sua resposta em aspectos de compras públicas e não nos forneceu informações sobre ameaças aos direitos humanos. Aparentemente, vendo nossa solicitação de informações como uma questão de responsabilidade, eles não abordaram nenhum risco aos direitos

humanos e usaram o fato de serem fornecedores, não usuários, da tecnologia para se distanciarem de qualquer impacto que os produtos possam ter.

A empresa brasileira **Intelbras** compartilhou respostas detalhadas tanto para nossas perguntas originais e como para as complementares. Embora tenham reiterado a importância de cumprir com as leis de proteção de dados, elas subestimaram a relevância de seu relacionamento comercial com a Dahua, empresa chinesa que detém 10% de seus negócios. A Intelbras afirmou que "não tem ligação ou responsabilidade pelas ações da empresa chinesa"; no entanto, como acionista, um representante da Dahua faz parte do conselho de administração da Intelbras. Isso significa que a Dahua tem a responsabilidade de garantir que seu investimento na Intelbras não contribua para danos aos direitos humanos, assim como a Intelbras deve garantir que os direitos humanos sejam respeitados em suas operações comerciais.

Tanto a empresa brasileira **Oi** (antiga Telmar) quanto a **Intelbras** argumentaram que os usuários finais (seus clientes) são os únicos responsáveis por como seus produtos ou serviços são usados. Enquanto isso, a **Dahua** disse que "não pode controlar totalmente como [suas] tecnologias são usadas pelos usuários finais". Essa narrativa ignora o fato de que a responsabilidade corporativa se estende por toda a cadeia de valor de uma empresa, com o UNGP 13 (b) afirmando que as empresas devem "procurar prevenir ou mitigar os impactos adversos aos direitos humanos que estão diretamente ligados às suas operações, produtos ou serviços por suas relações comerciais, mesmo que não tenham contribuído para esses impactos".

Operacionalmente, os esforços de devida diligência das empresas devem considerar os impactos sobre os direitos humanos, não apenas de seus produtos, mas também de quaisquer atividades relacionadas (UNGP 17 (a)). Quando as empresas não aceitam a responsabilidade pelos danos causados pela tecnologia que criam, elas limitam a capacidade de proteger a privacidade das pessoas afetadas por ferramentas com recursos de vigilância.

3. Cuidar dos clientes, mas não das pessoas impactadas

A resposta da **Oi** focou em como ela tem desenvolvido produtos e serviços alinhados à transformação digital e às tendências do mercado, mas não mencionou como eles protegem os direitos humanos. Isso contraria a exigência dos UNGPs de que as empresas assumam um compromisso político de respeitar os direitos humanos (UNGP 15) e de comunicar publicamente como lidam com os impactos de seus produtos ou serviços sobre estes direitos (UNGP 21).

A **Intelbras** prestou informações sobre o suporte pré e pós-venda que presta aos clientes e instaladores, bem como o seu compromisso de notificar "o usuário e as autoridades competentes" caso ocorra um "incidente envolvendo Dados Pessoais de usuários dos Serviços". No entanto, os riscos reais apresentados pelas tecnologias

com recursos de vigilância não são para os clientes que as implantam, mas para os indivíduos expostos a essas tecnologias. Portanto, o real ponto em questão é como as empresas limitariam os clientes do governo, especialmente aqueles com registros de violações de direitos humanos. Entretanto, a Intelbras desconsiderou isso em sua resposta, sugerindo que não avaliou os impactos de seus negócios sobre os direitos humanos, conforme exigido pelo UNGP 18.

4. Ter excesso de confiança em suas próprias políticas internas, apesar da falta de transparência

Em resposta à nossa pergunta sobre quaisquer políticas, protocolos ou processos internos que regem o fornecimento de soluções de vigilância pelas empresas a governos, várias empresas se referiram a suas políticas de licenciamento e privacidade de dados, termos de uso do produto e códigos de ética, assim como a regulamentos locais. Embora as políticas internas sejam um ponto de partida para a conformidade legal, elas não são suficientes para garantir a proteção dos direitos humanos. Como aponta o UNGP 16, "as empresas devem expressar seu compromisso de cumprir essa responsabilidade".

Por exemplo, a **Oi** compartilhou que atua "em todas as suas operações e projetos observando os mais altos níveis de governança, integridade, ética corporativa e respeito a todas as leis e regulamentos aplicáveis". Porém, eles não mencionaram o envolvimento com os direitos humanos ou os padrões internacionais.

A **Cellebrite** forneceu uma curta resposta por meio de uma empresa de relações públicas, descrevendo o tipo de produto vendido e afirmando que a empresa tem "políticas de licenciamento rígidas e restrições para regulamentar como os clientes utilizam [suas] soluções, e só vendem [sua] tecnologia para empresas, organizações, e agências que concordam em cumprir as rígidas políticas de licenciamento que regem seu uso adequado." No entanto, a empresa não forneceu detalhes sobre essas políticas, deixando a sociedade civil incapaz de monitorar ou verificar o cumprimento dos compromissos da empresa.

A **IBM** disse que emprega "processos rigorosos em [suas] operações globais para proteger contra compromissos comerciais diretos ou de terceiros que possam contrariar esses compromissos". Embora sua resposta completa estabeleça compromissos claros de acordo com os UNGPs, como condenar o uso de tecnologia para vigilância em massa e discriminação racial, a empresa não compartilhou nenhuma informação sobre o que são esses processos, nos impedindo de realizar uma análise completa e minuciosa.

A **NEC** foi mais longe, ao criar os Princípios de Direitos Humanos e IA do Grupo NEC para "demonstrar respeito pela privacidade e pelos direitos humanos em relação à aplicação e utilização de IA e dados biométricos em todos os negócios". No entanto, embora este grupo faça uma avaliação se seus produtos estão sendo usados para violar os direitos humanos, não há menção de qualquer canal para denúncia de

supostos abusos aos direitos humanos, tampouco fornecem detalhes sobre como quaisquer violações são avaliadas e tratadas (UNGP 20). A adesão aos direitos humanos deve ir além de um grupo de trabalho ou uma carta de princípios.

Em resumo, as empresas nos remeteram a políticas e princípios internos, códigos de ética ou grupos de trabalho – mas falharam em fornecer detalhes desses vários mecanismos ou informações específicas sobre como eles são implementados ou monitorados (UNGP 20).

A transparência total, detalhada e contínua é crucial para a proteção adequada dos direitos humanos, especialmente quando se tratam de parcerias público-privadas que permitem a implantação da tecnologia de vigilância. Os Estados têm o dever de proteger os direitos humanos, enquanto as empresas devem respeitá-los. As empresas devem, portanto, cumprir os padrões de transparência e devida diligência dos direitos humanos e fornecer informações suficientes para a sociedade civil e outros atores independentes para fins de responsabilização.

Access Now

www.accessnow.org

A Access Now defende e amplia os direitos digitais de pessoas e comunidades em risco. Como uma organização de base a global, estabelecemos parcerias com atores locais para levar uma agenda de direitos humanos para o uso, desenvolvimento e governança de tecnologias digitais e para intervir onde as tecnologias impactam negativamente nossos direitos humanos. Ao combinar suporte técnico direto, defesa estratégica, doações de base e reuniões como a RightsCon, lutamos pelos direitos humanos na era digital.

Para mais informações, queira contatar:

Ángela Alarcón
Campaigner, Latin America & the Caribbean
angela@accessnow.org