Óculos inteligentes, reconhecimento facial e a lacuna regulatória brasileira

09/06/2026

Uma jovem entra em uma academia, usa os equipamentos, conversa com o instrutor. Não sabe que está sendo filmada. O homem ao lado usa óculos que parecem comuns: são de marca famosa, discretos, sem qualquer sinal perceptível de gravação. Horas depois, ela aparece em um vídeo viral classificado como “pegadinha”. Tem milhões de visualizações. Descobre a exposição por mensagem de um amigo.

Esse episódio não é ficção científica. É o tipo de situação que já ocorre com frequência crescente nas redes sociais brasileiras e norte-americanas desde a popularização dos óculos inteligentes com câmera integrada. O debate público, porém, ainda permanece concentrado na camada mais visível do problema: discute-se o constrangimento individual, a exposição indevida, o limite entre humor e assédio. A questão mais ampla, contudo, é regulatória: a disseminação de dispositivos vestíveis com capacidade permanente de captação audiovisual, potencial integração com sistemas biométricos e ausência de parâmetros jurídicos específicos proporcionais aos riscos que representam.

Os óculos inteligentes mais conhecidos disponíveis no mercado integram câmeras embutidas nas hastes capazes de registrar fotos e vídeos em alta resolução com as mãos livres do usuário. O conteúdo pode ser transmitido ao vivo, armazenado digitalmente ou compartilhado instantaneamente em plataformas diversas. O dispositivo também incorpora assistentes de voz, microfones e conectividade permanente.

O principal mecanismo projetado para alertar terceiros é um pequeno LED externo que se acende durante as gravações. A suficiência desse alerta, contudo, já foi questionada por reguladores europeus — especialmente pela autoridade irlandesa de proteção de dados (DPC) e pelo Garante italiano —, diante da dúvida objetiva sobre sua efetiva perceptibilidade por pessoas ao redor [1].

A resposta informal do mercado foi mais rápida do que a regulatória: reportagens especializadas e pesquisa realizada pelos autores documentaram a comercialização de adesivos e modificações físicas destinados a neutralizar permanentemente esse sinal luminoso sem comprometer as demais funções do dispositivo. Os óculos, então, voltam a parecer simplesmente óculos comuns. Na prática, desaparece o principal mecanismo de aviso a terceiros.

Em outubro de 2024, os estudantes AnhPhu Nguyen e Caine Ardayfio, vinculados a Harvard, publicaram os resultados de um experimento que produziu desconforto relevante no setor de tecnologia. Batizado de I-XRAY, o projeto consistia em conectar o fluxo de vídeo dos óculos a ferramentas comercialmente disponíveis de reconhecimento facial e a bases públicas de dados pessoais [2].

O resultado demonstrou a plausibilidade técnica de identificar pessoas filmadas e correlacionar imagens com informações pessoais publicamente acessíveis — incluindo endereço residencial, número de telefone e dados de familiares, recuperados em cerca de noventa segundos a partir de uma imagem capturada pelas lentes [3]. O objetivo declarado não foi atacar um fabricante específico, mas evidenciar o que a convergência entre tecnologias já disponíveis comercialmente pode tornar possível.

Spacca

Os estudantes foram cuidadosos ao destacar que a demonstração não dependia exclusivamente daquele produto específico — em tese, lógica semelhante poderia ser aplicada a outros dispositivos com câmera. O ponto relevante, porém, é que a integração entre captação vestível, biometria e bases massivas de dados já deixou de ser hipótese meramente teórica [4]. A fabricante, segundo reportagens internacionais, chegou a considerar internamente funcionalidades relacionadas a reconhecimento facial, embora não as tenha implementado comercialmente.

Resposta regulatória internacional ainda é incipiente, mas já oferece pistas relevantes sobre a direção do debate

Na União Europeia, imagens de pessoas identificadas ou identificáveis podem constituir dados pessoais para fins do GDPR. Quando submetidas a tratamento biométrico destinado à identificação inequívoca do titular, podem ingressar no regime jurídico de dados sensíveis. O AI Act europeu, por sua vez, adotou postura significativamente mais restritiva em relação a sistemas de identificação biométrica remota, especialmente em determinados contextos de uso em espaços acessíveis ao público.[5]

Nos Estados Unidos, onde muitos dos vídeos virais desse tipo foram produzidos, a ausência de uma lei federal abrangente de privacidade limita a uniformidade regulatória. A captação de imagens em espaços públicos costuma receber proteção jurídica mais ampla. Ainda assim, organizações como a Electronic Frontier Foundation já alertaram que a combinação entre *smart glasses* e reconhecimento facial pode alterar profundamente expectativas sociais de privacidade [6].

No Brasil, a preocupação institucional com dispositivos de captação de imagem em contextos sensíveis já começou a emergir, ainda que de forma pontual. O problema estrutural, contudo, permanece sem enfrentamento normativo específico.

A Constituição protege expressamente a intimidade, a vida privada, a honra e a imagem das pessoas. O Código Civil restringe usos indevidos da imagem. A Lei Geral de Proteção de Dados disciplina o tratamento de dados pessoais, inclusive biométricos nas hipóteses legalmente previstas.

Esses instrumentos existem. O problema está nas lacunas que a tecnologia wearable expôs e que nenhum deles enfrenta de modo direto.

Hoje, não há disciplina legal específica e claramente estruturada para dispositivos vestíveis com captação audiovisual contínua. Não existe obrigação legal expressa de mecanismos padronizados e eficazes de aviso a terceiros. Não há tratamento normativo específico para a neutralização deliberada desses mecanismos. Tampouco existe disciplina regulatória clara para uso privado de reconhecimento facial acoplado a *wearables* em espaços públicos.

Nem toda gravação realizada em espaço público é, por si só, ilícita. O problema jurídico depende do contexto, da finalidade, da forma de captação, da exposição indevida e do potencial abuso contra direitos da personalidade e proteção de dados.

A gravação de pessoa sem consentimento em situação que exponha nudez, intimidade sexual ou conteúdo de natureza semelhante pode configurar ilícitos específicos, inclusive penais. Mas grande parte das chamadas “pegadinhas” virais permanece aquém desse limiar, o que não as torna juridicamente indiferentes, mas frequentemente dificulta respostas rápidas e efetivas antes da disseminação do dano.

A viralização desse tipo de conteúdo é apenas a manifestação mais visível de uma questão regulatória mais ampla: a assimetria entre a capacidade tecnológica de vigilância privada e a ausência de parâmetros jurídicos proporcionais ao potencial de dano.

Algumas medidas merecem debate sério

A exigência legal de mecanismos visíveis e tecnicamente robustos de aviso durante gravações por dispositivos vestíveis parece um ponto de partida razoável — um caminho que reguladores europeus já percorrem, ainda que com resultados parciais [7]. Também parece legítima a discussão sobre limites jurídicos claros para integração entre *wearables* e sistemas de identificação biométrica remota em espaços públicos, especialmente em usos privados não supervisionados.

A ANPD pode ter papel relevante nesse debate, especialmente quanto a deveres de governança, transparência e mitigação de riscos associados ao tratamento de dados decorrente desses ecossistemas tecnológicos.

As plataformas que hospedam e amplificam esse tipo de conteúdo também não podem permanecer fora da discussão regulatória. É legítimo debater regimes mais claros de responsabilização quando, após ciência inequívoca da ilicitude, mantêm circulação de conteúdo obtido mediante captação abusiva da imagem de terceiros.

O problema dos óculos inteligentes não é tecnológico. A tecnologia já existe, já escala e já chegou ao Brasil. O problema é jurídico e institucional: saber se o ordenamento brasileiro está preparado para lidar com dispositivos capazes de ampliar significativamente a identificação silenciosa de pessoas em espaços públicos.

---

[1] Ireland's Data Protection Commission (DPC) e Garante italiano questionaram, já em 2021, a eficácia do LED como mecanismo de aviso, exigindo que a Meta demonstrasse sua perceptibilidade em campo. Veja: https://www.dataprotection.ie/en/news-media/latest-news/data-protection-commission-statement-concerning-facebook-view-glasses

[2]NGUYEN, AnhPhu; ARDAYFIO, Caine. I-XRAY: projeto de demonstração pública sobre reconhecimento facial acoplado a óculos inteligentes. Harvard University, set./out. 2024. Cobertura jornalística: https://www.bostonglobe.com/2024/10/04/business/harvard-students-ai-meta-glasses/

[3]ARDAYFIO, Caine, citado em: TECHSPOT. "Harvard students create smart glasses that instantly dox strangers". 3 out. 2024. Disponível em: https://www.techspot.com/news/104973-harvard-students-create-smart-glasses-instantly-dox-strangers.html

[4]Harvard Technology Review. "AI Glasses Unveil Privacy Risks: An Interview with the Creators of I-XRAY". 1 nov. 2024. Disponível em: https://harvardtechnologyreview.com/2024/11/01/ai-glasses-unveil-privacy-risks-an-interview-with-the-creators-of-i-xray/

[5]Regulamento (UE) 2016/679 (GDPR), art. 9.º. Regulamento (UE) 2024/1689 (AI Act), arts. 5.º e 10.º e ss., sobre identificação biométrica remota em espaços públicos.

[6]Electronic Frontier Foundation. Declarações públicas sobre smart glasses e reconhecimento facial, 2023-2024. Disponível em: https://www.eff.org

[7]Ireland's DPC questionou a eficácia do LED e, em resposta às pressões regulatórias, a empresa ampliou o indicador luminoso e adicionou padrão piscante. Cf. ANZOLIN, Elisa; LO NOSTRO, Gianluca. "Ray-Ban Meta glasses take off but face privacy and competition test". Reuters/AOL, dez. 2024. Disponível em: https://www.aol.com/articles/ray-ban-meta-glasses-off-161528951.html