Do roubo de imagens aos deepfakes: a nova fronteira da manipulação digi

Data: 2025-09-15 06:30:02

Autor: Inteligência Against Invaders

Paolo Galdieri**:15 setembro 2025 07:58**

Nos últimos meses, tenho repetidamente me encontrado apresentando reclamações sobre vídeos falsos que circulam online. Não estamos falando apenas de conteúdo roubado distribuído sem consentimento, mas também de deepfakes: vídeos em que rostos famosos são sobrepostos a corpos estranhos, muitas vezes usados para promover investimentos financeiros ou inseridos em contextos pornográficos.

Um fenômeno que, infelizmente, não surpreende mais por sua presença, mas pela velocidade com que cresce, se espalha e melhora.

De sites “amadores” a falsificações digitais: um continuum de abuso

Aqueles que seguem a indústria aprenderam sobre plataformas como Mia moglie ou Phica. Plataformas onde a aparente espontaneidade muitas vezes esconde um verdadeiro mercado para os corpos e intimidades de outras pessoas. Em muitos casos, os vídeos são enviados sem o consentimento das pessoas retratadas. Gravações privadas são roubadas ou o conteúdo compartilhado em um momento de confiança de repente se torna de conhecimento público.

1. L’acquisto del fumetto sul Cybersecurity Awareness
2. Ascoltando i nostri Podcast
3. Seguendo RHC su WhatsApp
4. Seguendo RHC su Telegram
5. Baixar gratuitamente “Dark Mirror”, il report sul ransomware di Dark Lab

Se ti piacciono le novità e gli articoli riportati su di Red Hot Cyber, iscriviti immediatamente alla newsletter settimanale per non perdere nessun articolo. La newsletter generalmente viene inviata ai nostri lettori ad inizio settimana, indicativamente di lunedì.

O próximo salto tecnológico é representado por deepfakes. Se em sites amadores o problema era (e é) o roubo de imagens reais, hoje a fasquia é ainda mais elevada: não é mais necessário roubar um arquivo; Uma fotografia é suficiente para criar um vídeo no qual a pessoa parece fazer ou dizer algo que nunca fez. É a transição da violação da privacidade para a criação de uma realidade verdadeiramente alternativa.

Rostos famosos e rostos comuns: duas vulnerabilidades diferentes

O impacto dessas manipulações varia dependendo de quem é a vítima.

Rostos famosos – atores, políticos, influenciadores – são um alvo privilegiado: sua exposição pública facilita a descoberta e a exposição de notícias falsas, mas ao mesmo tempo amplifica os danos, pois elas se espalham muito rapidamente e em grande escala.

Para rostos comuns, no entanto, a situação é ainda mais insidiosa. Sem a mesma visibilidade, eles também não têm meios para se defender: é improvável que consigam monitorar a internet ou obter a remoção oportuna de conteúdo. Nesses casos, o engano costuma ser mais confiável, precisamente porque não há “original” de domínio público para comparar o falso. A consequência é devastadora: pessoas comuns se veem envolvidas em vídeos sexuais manipulados ou falsas promoções financeiras, com efeitos destrutivos em suas vidas privadas e profissionais.

Os regulamentos precisam ser atualizados

Diante dessa realidade em constante evolução, a lei muitas vezes parece ficar atrás da tecnologia. A tradição jurídica italiana já introduziu regras importantes, mas os deepfakes escapam problematicamente às categorias jurídicas tradicionais. As imagens de origem podem ser públicas e o conteúdo manipulado não se limita à pornografia, mas também à desinformação financeira, política ou relacionada à saúde. No entanto, os danos à pessoa invoLVED são comparáveis – e em alguns casos até piores – do que os já cobertos.

Por conseguinte, a introdução de legislação específica pode ser uma resposta necessária. O objetivo não é multiplicar as acusações criminais, mas identificar uma disposição e circunstâncias agravantes específicas relacionadas ao uso de inteligência artificial para manipular a imagem e a voz de um indivíduo. O Projeto de Lei nº 1146/2024, que dedica um artigo às disposições criminais, adota essa abordagem. O projeto de lei introduz um novo crime, a “divulgação ilícita de conteúdo gerado ou alterado com sistemas de inteligência artificial”, punível com pena de prisão de um a cinco anos

para quem divulgar, sem consentimento, imagens, vídeos ou vozes manipuladas artificialmente capazes de induzir em erro. Além disso, o projeto de lei prevê uma série de circunstâncias agravantes comuns e específicas: fraude, fraude informática, lavagem de dinheiro, autolavagem, manipulação de mercado e até falsificação de identidade podem ser punidas com mais severidade se cometidas com o uso de ferramentas de inteligência artificial. Trata-se, portanto, de uma tentativa de atualizar o Código Penal, sem criar um corpus independente, mas fortalecendo as ferramentas existentes quando a IA se torna um meio de atividade criminosa.

A nível europeu e internacional, o debate já está aberto: basta pensar na Lei da IA em discussão em Bruxelas, que procura estabelecer regras comuns para os sistemas de inteligência artificial, incluindo os riscos de manipulação audiovisual.

Desafios abertos: tecnologia, direito, cultura

A luta contra deepfakes e vídeos roubados não pode ser vencida com uma única ferramenta, mas com a sinergia de múltiplos planos de intervenção. O desafio tecnológico. Precisamos de algoritmos capazes de identificar automaticamente o conteúdo manipulado e sinalizá-lo antes que se torne viral. Algumas universidades e centros de pesquisa estão desenvolvendo marcas d'água digitais e sistemas de rastreamento de imagem para distinguir o autêntico do falso. No entanto, é uma corrida sem fim: cada nova ferramenta de detecção estimula o surgimento de técnicas de falsificação mais sofisticadas. O desafio é, portanto, contínuo e requer investimentos públicos significativos, não deixados apenas para interesses privados.

O desafio legal. Além dos regulamentos, procedimentos eficazes são cruciais. Uma vítima que descobre um deepfake em uma plataforma internacional não pode esperar meses para obter sua remoção. São necessários canais de emergência, semelhantes aos introduzidos para conteúdo terrorista online, que permitem que as autoridades solicitem exclusão imediata e vinculativa. Ao mesmo tempo, é necessário fortalecer a cooperação internacional, porque os servidores estão frequentemente no exterior e os responsáveis operam em países com legislação menos rigorosa.

O desafio cultural. Este é provavelmente o jogo mais decisivo. Uma sociedade que não consegue distinguir a verdade da falsidade está destinada a se tornar um terreno fértil para manipulação de todos os tipos, desde fofocas até propaganda política. Precisamos de educação digital nas escolas, programas de alfabetização de adultos e campanhas institucionais que expliquem os riscos e ensinem a reconhecer conteúdos manipulados. A consciência crítica é o melhor antídoto para a viralidade das falsificações.

Um desafio para a civilização

O fio condutor que liga sites amadores como Mia moglie e Phica aos deepfakes mais sofisticados é sempre o mesmo: o uso não consensual da imagem e identidade de uma pessoa. Hoje, não se trata mais apenas de um problema relacionado à pornografia ou à morbidez de certos contextos, mas de uma questão que diz respeito à democracia, à economia e à convivência civil.

Se alguém puder criar um vídeo confiável com o rosto de um político declarando guerra, um empresário convidando o investimento em um golpe ou uma pessoa comum atraída para um cenário pornográfico, a confiança na própria realidade será prejudicada. Não é mais apenas uma questão de proteger reputações individuais, mas de preservar a coesão social e a capacidade de distinguir o que é real do que é construído artificialmente.

Nesse sentido, o combate aos deepfakes e à disseminação de vídeos roubados representa um verdadeiro desafio para a civilização. Direito, tecnologia e cultura não são suficientes: precisamos de uma aliança que os reúna, envolvendo instituições, plataformas e cidadãos. Não está apenas em jogo a dignidade dos indivíduos, mas a qualidade de nossa vida democrática.

Paolo Galdieri
Advogado criminal, também conhecido como professor de Direito Penal da Tecnologia da Informação, ocupou cargos acadêmicos importantes, incluindo a coordenação didática de um mestrado de nível II na La Sapienza em Roma e atribuições de ensino em várias universidades italianas. É autor de mais de uma centena de publicações sobre direito penal cibernético e participou de importantesconferências internacionais como representante sobre o tema do crime cibernético. Além disso, colaborou com organizações e programas de televisão, dando o seu contributo especializado em cibercrime.

Lista degli articoli
Visita il sito web dell’autore