Europol Report Criminal Use of Deepfake Technology

Cornelia Riehle

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Cornelia Riehle
Deputy Head of Section
Academy of European Law

ISSN: 1862-6947
https://eucrim.eu

On 28 April 2022, Europol's Innovation Lab published its first report giving a detailed overview of the criminal use of deepfake technology. The phenomena of deepfakes, the technology behind them, deepfake technology's impact on crime and on law enforcement, the detection of deepfake, and actions e.g. by technology companies and the EU to respond to deepfakes are explained in six chapters.

Employed properly, deepfake technology can produce content that convincingly shows people saying or doing things they never did or create people that never existed in the first place. Regarding the technologies behind deepfakes, the report stressed that the adaptation of generative adversarial networks (GANs) - a mechanism designed to minimise the chance products can be discriminated from the authentic content – a great leap in the quality and accessibility of deepfake technology. Furthermore, the growing evolvement of crime as a service (CaaS) in parallel with such technologies is of increasing concern for law enforcement. Deepfake technology can facilitate various criminal activities, *inter alia*:

- Harassing or humiliating individuals online;
- Perpetrating extortion and fraud;
- Facilitating document fraud;
- Falsifying online identities and fooling "know your customer" mechanisms;
- Non-consensual pornography;
- Online child sexual exploitation;
- Falsifying or manipulating electronic evidence for criminal justice investigations;
- Disrupting financial markets;
- Distributing disinformation and manipulating public opinion;
- Supporting the narratives of extremist or terrorist groups;
- Stoking social unrest and political polarisation.

Alternately, deepfake technologies have an impact on police work and the legal process as deepfake material requires more qualified assessment and cross-checking and new methods of detection. Hence, the report sees a strong need to adapt the regulatory frameworks - from laws to policies and practices. Law enforcement, online service providers and other organisations need to develop their policies and invest in detection and prevention technology. Policymakers and law enforcement agencies need to evaluate their current policies and practices, and adapt them to be prepared for the new reality of deepfakes. New legislation should therefore set guidelines, enforce compliance, and support law enforcement preparedness efforts.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by the European Union