

Zooming in on AI: tackling deepfakes around the world

 FROM OUR BLOG

A&O Shearman on technology

READ TIME

 20 mins

PUBLISHED DATE

 Aug 14 2025

Deepfakes (also known as digital replicas) are created when sophisticated AI technology generates or alters audio-visual content to misrepresent someone or something. Often a person's voice or appearance is digitally manipulated or replicated and methods such as lip syncing or face swapping can create realistic synthetic media that convincingly depicts the individual saying or doing things that they never actually did.

Over the past few years, the widespread availability of deep learning technology and the resulting proliferation of convincing deepfakes has raised significant concerns, not only across various commercial sectors but also for private individuals. Deepfakes blur the line between reality and fabrication and can quickly spread misinformation and disinformation, thereby undermining public trust and even the democratic process. Digital

replicas can deceive and bypass voice and facial recognition security measures, trick vulnerable employees into divulging confidential information, clone voices (potentially eliminating the need for human performers) and cause personal and reputational harm, such as through explicit deepfake imagery and identity theft.

Deepfakes are a real concern, but it is not an easy task to tackle them effectively around the world. There is currently a complex and inconsistent patchwork of legal measures, which need to be applied to the circumstances of a particular deepfake. This article reviews the current laws in China, the U.S., UK and Germany, the notable gaps and limitations, and the potential legal reforms being contemplated to enhance protection in this area.

Note that this article only discusses how to tackle deepfakes which are intended to mislead and be taken as the truth and not those that are obviously recognizable as an imitation, used for satirical or advertising purposes and/or possibly covered by exceptions such as freedom of expression, freedom of the press and parody. It also doesn't deal with the legitimate use of synthetic media in, e.g., marketing and advertising. Please see our [previous article](#) for a discussion of the IP opportunities and risks posed by generative AI that synthesizes and manipulate marketing content.

Specific laws regulating AI-generated content and deepfakes

Laws that specifically target AI-generated content and deepfakes vary widely across different jurisdictions. China has the most comprehensive regulatory framework for AI-generated content, specifically banning the distribution of AI-generated fake news and mandating notice and consent from any individual whose biometric information is edited to create a deepfake. In China and the EU, all AI-generated media including deepfakes need to be labelled as such, with a view to identifying non-genuine content and minimizing confusion.

On the other hand, the laws in the U.S. and UK only concern specific types of digital replicas. The U.S. has little federal legislation, leaving the issue mostly

to state-level laws which regulate specific types of content, e.g., audio or election propaganda. Similarly, the UK only has a specific law dealing with the narrow (but important) subset of sexually explicit deepfakes.

Given the evident need for more comprehensive regulation to address broader concerns, it is likely that we will see the introduction of additional laws in the future.

China

- ◆ It is illegal¹ to produce, reproduce, publish, or disseminate prohibited information and fake news through AI.
- ◆ When editing biometric information like facial features and voices, the individuals whose information is being edited should be informed and their separate consent should be obtained².
- ◆ The provision and use of generative AI services should respect rights in IP and personal information³.
- ◆ Specific regulations on how content generated and synthesized by AI should be marked⁴ will come into effect later this year.

UK

- ◆ The UK's only laws in this area concern sexually explicit deepfakes. It is currently illegal⁵ intentionally to share photographs or film without the subject's consent, which show or appear to show another person in an intimate state. There are also ongoing proposals for a new offense⁶ of creating a sexually explicit deepfake without consent.

U.S.

- ◆ There is no comprehensive U.S. federal legislation regulating AI and deepfakes, although recently Congress passed the TAKE IT DOWN Act,⁷ which provides some limited protection against non-consensual intimate AI-generated content. There are, however, a variety of state laws in this

area. For example:

- ◆ Tennessee: There is civil liability⁸ for unauthorized audio deepfakes.
- ◆ California: There is a cause of action⁹ for unauthorized commercial use of a deceased's personality. Further, three bills have been signed¹⁰ into law to combat the use of deepfakes in election campaigns by requiring platforms to remove or label such content and mandating clear disclosures on political ads that use AI-generated media.
- ◆ Texas: It is a criminal offense¹¹ to use deepfakes with the intent of injuring an election candidate or influencing the outcome of an election.

EU

- ◆ The AI Act requires labelling of AI-generated content:
 - ◆ providers of AI systems that generate synthetic audio, images, videos or text are required¹² to label any output as artificially generated or manipulated;
 - ◆ deployers of AI systems that generate deepfakes are required¹³ to disclose that the content has been artificially generated or manipulated;
 - ◆ very large online platforms and very large online search engines are required¹⁴ to label deepfakes if users could mistakenly believe them to be genuine.

Personality, publicity or image rights

These rights generally protect against an individual's persona: their personality, image, voice, name or likeness. As such, they can play a crucial role in safeguarding against misuse of an individual's appearance or voice in a deepfake. The potential for use and commercialization of voice cloning independently of its wearer also necessitates protection.

The extent of protection afforded to these rights again varies across jurisdictions. In Germany, there is protection for both image and voice rights, and in China courts have already ruled that deepfaking by face swapping is

an infringement of image rights. In the UK, such rights are not explicitly protected but passing off may provide effective protection in some circumstances. Again, the degree of protection in the U.S. varies by state.

UK

- ◆ The courts have specifically stated that image rights are not explicitly protected in the UK¹⁵. However, a passing off action (see more details below) could succeed against a deepfake that misrepresents that a well-known individual is endorsing a particular product. The claimant needs to have goodwill (the attractive force that brings in business), there needs to be a false endorsement, and the individual needs to have a previous reputation for endorsing products and services¹⁶. This can therefore be an effective way to protect a famous person's image but in restricted circumstances.
- ◆ The court has not yet given a definitive ruling on voice rights i.e. whether the unauthorized use of a voice for commercial gain would constitute passing off. Some judges have hinted that they think it should.¹⁸

China

- ◆ Personality rights, including image rights, are protected and there is a specific prohibition¹⁹ on “infringing upon others’ image rights by means of falsification through information technology and other methods”. Deepfaking the image of others on an AI face-swapping app has been held to constitute an infringement of image rights.
- ◆ Voice rights are also protected²⁰. Deepfaking the voice of others has been held to constitute an infringement of voice rights if a natural person could be identified through a synthetic voice.

Germany:

- ◆ Right in own image: images may only be distributed or publicly displayed with the consent of the person depicted²¹. It hasn't yet been confirmed

that this covers deepfakes, but it should include any recognizable reproduction of a person's appearance.

- ◆ Right to own voice: whilst this is not expressly protected, it is likely protected²² by way of analogy.
- ◆ General personality rights: protect²³ against the distribution of a technically manipulated image that appears to be an authentic depiction of a person. This applies to living individuals as well as post-mortem.

U.S.

- ◆ Some states provide rights in a person's voice or likeness and protect against unauthorized commercial use and appropriation of an individual's persona. Protection varies by state (i.e. specific laws, invasion of privacy claims or common law). Approximately 38 states recognize a right of publicity but only a subset of them (approximately 23) recognize this right post-mortem, with varying degrees of protection.
- ◆ It is therefore important to analyze the laws of each state to determine their applicability to a given dispute involving a deepfake.

Copyright, performance and moral rights

Sound recordings, photos or films used to create a deepfake may be protected by copyright. If a substantial part of such a work is copied, manipulated or adapted to create the deepfake (e.g., a new face is added to an existing image), this may give rise to copyright infringement, in addition to other infringements arising from the subsequent publication of the deepfake²⁴.

It is not yet clear how exceptions to infringement will apply to deepfakes. In the EU and UK, there is a fair dealing exception for parody²⁵ but this is more likely to cover, for example, humorous memes rather than true deepfakes (i.e., those intended to be taken truthfully) or those that interfere with the market for the original work.

There is a broader fair use doctrine in the U.S.²⁶, which is assessed on a

case-by-case basis, weighing four statutory factors: the transformative nature and purpose of the use (including whether it is commercial or non-commercial), the nature of the copyrighted work, the amount and substantiality of the portion used, and the effect of the use on the potential market for or value of the original work. Recent guidance in a report from the U.S. Copyright Office²⁷ clarifies that fair use in the context of AI training is not automatic, especially when models generate expressive outputs that compete with or substitute for originals, posing significant risks to market harm, lost sales, and lost licensing opportunities. Whether fair use applies in such cases has been the subject of recent opposing U.S. court decisions. However, deepfakes created through the unauthorized wholesale, commercial copying of expressive works subject to copyright protection may infringe and are unlikely to succeed on a fair use defense. China's narrow fair use defense²⁸ is unlikely to apply as it only covers specific non-commercial scenarios in the public interest, such as if the deepfake comprises a translation, adaptation or compilation of a published work for the use of teachers or researchers in the context of education and scientific research.

In any event, copyright has some limitations. It protects the expression of original subject matter (photographs, paintings, sound recordings and films) but not the identity, voice or image itself. This means that, if the deepfake merely mimics or synthesizes a person's likeness or voice without reproducing any protectable expression from a copyrighted work, it will generally fall outside the scope of copyright infringement. Furthermore, any action needs to be taken by the copyright owner. In a lot of cases, this will be, e.g., the photographer or the producer of the original sound recording or film and not necessarily the person who is harmed by being depicted in the deepfake.

Performance rights

In the UK, U.S. and China, there are separate performance rights that protect against the unauthorized copying of a substantial part of a performance recording. As such, they could be relevant to deepfakes that clone the voices of performers such as recording artists and musicians. However, in their current form, these rights only prevent the making of a copy of the

recording of a performance and will therefore not assist if the AI can synthesize or imitate a performance without creating a copy of the original recording. In Germany, the right of the performing artist²⁹ prevents the distortion or manipulation of the performance of an artist but not, for example, speeches of a politician. It is highly questionable, though, whether these rights help against a deepfake that does not imitate or copy a specific performance, such as a specific ballet dance or band concert, but only uses the likeness of certain artists to create a made-up performance that never happened in real life.

Moral rights

In the UK, China, and Germany, any deepfake that distorts an original copyright work may infringe the author's moral right of integrity, i.e., to object to derogatory treatment of the work³⁰. Similarly, performers may object if a deepfake distorts, mutilates or otherwise modifies a sound recording of their performance in a way that is prejudicial to their reputation. However, if a deepfake does not unlawfully copy or distort a copyrighted work that existed before (be it a movie scene, a choreography, a photograph, a poem, or the like) but simply uses someone's likeness to create something new, this would not be covered. Instead, in the UK, if the deepfake conveys to a reasonable viewer an unequivocal false statement that someone was the author or director, this may be covered under the moral right not to have a work falsely attributed to you as author³¹.

In the U.S., moral rights are more limited in scope and primarily relate to the right of attribution (the right to be credited as the author) and the right of integrity. The U.S. Copyright Office recognizes that the harms caused by unauthorized digital replicas can closely resemble violations of moral rights. Specifically, non-commercial harms like reputational damage or misattribution are similar to the moral rights of attribution and integrity.

Trademarks

In order to strengthen protection against unauthorized use of their features, people may try to acquire trademark protection for their image, gestures or

even their voice. This raises novel issues and the EUIPO Grand Board of Appeal is due to consider whether an image of a person's face is capable of functioning as a trademark³².

If an individual manages to secure a trademark registration for their name, image or voice, it may be an infringement to use it in the creation of a deepfake without permission³³. However, this is limited to circumstances when the deepfake is used commercially i.e. in the course of trade and, in most circumstances, in relation to goods and services that are similar to those that are protected, such that there is customer confusion. It may be difficult for less famous individuals to prove that the challenged conduct is likely to confuse consumers and, as an example, AI-generated “revenge porn” is unlikely to be covered.

There is also extended protection for marks with a reputation (or famous marks) if the deepfake causes detriment, tarnishes the mark's reputation, or takes unfair advantage of the mark. This could be relevant, for example, to deepfakes that are likely to raise unpleasant associations because they are linked to drugs, sex or crime. However, again this requires use in the course of trade and is likely to be limited to famous individuals.

Unfair competition/passing off

While deepfakes are often associated with entertainment or political manipulation, they can also pose risks to businesses if they are used to deceive consumers and misrepresent commercial endorsements or affiliations. Such deceptions can severely impact brand reputation and consumer trust.

Protection against these types of deception differs depending on the jurisdiction, although they usually only apply in a commercial or competitive context when consumers are confused. As such they can't address other harms that can be inflicted by non-commercial uses, including deepfake pornography.

- ◆ A passing off action may assist against deepfakes if it can be proven that (i) the person depicted has goodwill (the attractive force that brings in business); (ii) there is a misrepresentation such as a clear false attribution of its content such that rational people are misled; and (iii) this is likely to cause damage³⁴.

U.S.

- ◆ There is a prohibition³⁵ on unfair or deceptive acts in interstate commerce, which can encompass misleading uses of an individual's identity. However, this only applies to unfair acts in commerce (and not non-commercial contexts).
- ◆ There are various state deceptive business practice laws that would prevent uses of deepfakes that are deceptive or cause consumer confusion.

China

- ◆ Deepfakes may constitute unfair competition but only if there is confusion i.e. consumers are misled into believing that products/services are those of others or that there is a specific connection with others³⁶.

Germany

- ◆ Deepfakes used for commercial purposes, such as misleading advertising, can be considered unfair competition³⁷. A competitive relationship is required i.e. the individual or company that uses the deepfake must do so in order to compete for market share (such as a deepfake showing the CEO or a brand ambassador of a certain company endorsing a competitor's product). It is sufficient, though, if the person creating or publishing a deepfake does so in order to support a third party with such a competitive relationship.

Advertising rules

The emergence of deepfakes poses unique challenges in advertising. Synthetic media is inherently artificial and capable of misleading consumers. Indeed, the purpose of many deepfakes is to distort reality. In some countries, such as the UK, there is an independent advertising regulator who can receive complaints and take action against misleading advertising, and in China this function is undertaken by a department under the State Administration for Market Regulation. In Germany, however, such matters need to be dealt with by the courts under unfair competition laws. The U.S. has various state false advertising laws that specifically protect against misleading political communications.

UK

- ◆ Deepfakes used in advertising directed at consumers must not “materially mislead or be likely to do so”³⁸. These advertising rules are enforced by the Advertising Standards Authority.

U.S.

- ◆ There are various state false advertising laws that deceptive deepfakes may violate. For example, Oregon mandates³⁹ disclosures for synthetic media in election campaigns, while Indiana requires⁴⁰ disclaimers for fabricated media in election communications. These laws aim to protect consumers from misleading information and ensure transparency in advertising and political communications involving deepfakes.

China

- ◆ Advertisements shall not “contain false or misleading content” and shall not “deceive or mislead consumers”⁴¹. It is also illegal⁴² to “conduct false or misleading commercial publicity regarding products”. The law on advertising is enforced by the State Administration for Market Regulation.

Germany

- ◆ Misleading advertising is dealt with as unfair competition (as above), which requires a competitive relationship. There is no regulator to enforce this, so it remains a matter for competing businesses, consumer bodies or industry associations to take to court.

Data protection

Where a photo or video relates to an identified or identifiable individual (through facial features, body language or a voice), this constitutes personal data in the UK, EU, and China⁴³. Adapting or altering such a photo or video to create a deepfake is therefore likely to constitute the processing of personal data⁴⁴. Accordingly, and amongst other things, a lawful basis (e.g., consent of the data subject, legitimate interest etc) is required⁴⁵ and the processing needs to be conducted in accordance with a number of principles (including for example lawfulness, fairness, transparency and accuracy). To the extent a facial image constitutes biometric data, processing requirements may also be more stringent⁴⁶. Furthermore, there is also potential criminal liability for example in Germany, for the creation of deepfakes in a private, but not political, context⁴⁷.

In practice, when considering the malicious use of deepfakes (e.g., when used to mislead), it is difficult to see how data protection compliance can be successfully achieved.

Other laws

To complicate matters further, these jurisdictions have a host of additional potential causes of action that may be triggered by deepfakes used in different circumstances. For example, there is defamation in the UK⁴⁸, China⁴⁹ and Germany⁵⁰ if a deepfake portrays an individual in a false and damaging way and is likely to cause serious harm to that person's reputation (e.g., confessing to a criminal act). Similarly, there is the potential for fraud in the UK, Germany⁵¹, and China⁵² if, for example, a party is induced to dispose of assets because of identity theft or a romance scam. Other possible causes of action include:

- ◆ (UK) Harassment:⁵³ if the use of the deepfake involves a course of conduct (two or more occasions), causing the victim distress or alarm (e.g., bullying or online abuse)
- ◆ (UK) Malicious Falsehood: if the deepfake is false, made maliciously and contains words that refer to a person, property or business and result in financial loss to the victim
- ◆ (UK) Misuse of Private Information⁵⁴: if fake footage constitutes an intrusion into personal space where the subject would have a reasonable expectation of privacy⁵⁵
- ◆ (Germany) German Civil Code (BGB):⁵⁶ if someone uses a deepfake intentionally to harm someone in an immoral manner
- ◆ (Germany) German Criminal Code (StGB):
 - ◆ if a deepfake “confesses” to criminal acts that were not committed⁵⁷
 - ◆ insult, if the depiction is likely to make the person depicted contemptible (verächtlich)⁵⁸
 - ◆ violation of intimate privacy⁵⁹ if picture material is manipulated in a way that significantly damages the reputation of the person depicted, though it remains unclear whether completely newly created picture material would fall under these provisions
- ◆ (China) The crime of fabricating and deliberately spreading false information:⁶⁰ if a deepfake containing false information (such as false disaster reports) is published online and seriously disrupts social order.

Practical issue: anonymity and intermediaries

One of the significant practical challenges in combating deepfakes is the difficulty in identifying the creators of such content. Deepfakes can be produced and disseminated anonymously, making it nearly impossible to trace the originator. This anonymity severely restricts efforts to hold the responsible parties accountable. Consequently, removal of content must

often be sought through, e.g., the notice and take down procedures of social media platforms and other intermediaries. However, this does not prevent the content from re-appearing elsewhere and victims having to play “whack-a-mole” to keep the content down⁶¹.

The effectiveness of these measures largely depends on the responsiveness of the platforms and the clarity of the legal framework governing intermediary liability and content removal. In the U.S., online providers are generally shielded from liability for content provided by third parties including deepfakes⁶² if they act upon receiving a valid notice of infringing content. Similarly, in the UK, EU and China, online intermediaries are protected from liability for third party content that they host or transmit provided that they act swiftly to remove it once they become aware of its illegality⁶³. Furthermore, China and the EU mandate providers of hosting services to provide pre-defined notice and action mechanisms for illegal content⁶⁴.

This should incentivize the platforms to act quickly after receiving a clear and effective notice of illegal content. Social media platforms also have their own policies on removing misinformation, particularly if it causes harm to individuals or society or contains the likeness of people without their permission. Due to the scale and speed of deepfake dissemination, we may start to see platforms introducing new technology (e.g., facial recognition technology) to help detect scams.

Proposals for reform

Because of the limitations and gaps in legal protection against digital replicas identified in this article, countries are starting to look at potential law reforms:

- ◆ The previous German government proposed the introduction of a new criminal offense⁶⁵ for breaching personality rights by a deepfake. It is unclear whether, and to what extent, the new government will resume this draft bill.
- ◆ Several deputies from the Chinese legislature (the National People’s

Congress or NPC) have suggested⁶⁶ enhancing regulations on deepfakes and expediting the legislative process for a dedicated law on deepfakes. It remains to be seen how the government and the NPC will respond to these suggestions.

- ◆ As part of its ongoing consultation on AI and copyright, the UK government is seeking views as to whether existing laws are sufficient to protect against deepfakes or if further legislative intervention is required.
- ◆ The U.S. Congress is considering several legislative proposals:
 - ◆ The No AI FRAUD Act and NO FAKES Act include provisions for balancing public interest against private rights, statutory damages, and attorney's fees.
 - ◆ The DEEPFAKES Accountability Act mandates digital watermarks for deepfake content and criminalizes malicious deepfakes.
 - ◆ The Preventing Deepfakes of Intimate Images Act allows civil suits for unauthorized intimate digital depictions.
 - ◆ The Copyright Office has advocated for a new federal law that protects all individuals from the knowing distribution of unauthorized digital replicas. This should protect realistic digital replicas of all individuals, enforce liability for unauthorized distribution, balance free speech, provide remedies, and coexist with state laws without full federal pre-emption.

Conclusion

Deepfakes are a real concern but tackling them in an effective and efficient manner around the world is problematic. There is a complex patchwork of inconsistent legal measures that need to be analyzed and applied to the circumstances of a particular deepfake.

Existing laws have notable restrictions and often provide sufficient redress for those harmed by digital replicas. Image or personality rights that protect an individual's persona are not uniform. Copyright protects original works but not an individual's image or voice alone. Unfair competition and

trademark laws only apply to commercial acts and often require consumer confusion so are unlikely to assist less well-known individuals. In practice, when considering the malicious use of deepfakes, it is difficult to see how data protection compliance can be successfully achieved.

Governments around the world are therefore considering potential reforms to strengthen their legal frameworks in this area. The speed, precision, and scale of AI-created digital replicas that we are now experiencing may necessitate legislative changes in the very near future.

Footnotes

1 The Regulations on the Administration of Deep Synthesis of Internet Information Services

2 Ibid

3 Interim Measures for the Administration of Generative Artificial Intelligence Services

4 The Measures for Marking Artificially Intelligent Generated and Synthesized Content

5 s188 Online Safety Act 2023 created a new s66B of the Sexual Offences Act 2003

6 Crime and Policing Bill

7 S.146 - TAKE IT DOWN Act

8 Ensuring Likeness, Voice, and Image Security (ELVIS Act)

9 California's AB 1836

10 California's AB 2655, AB 2839, and AB 2355

11 SB 751

12 Art. 50.2 of the EU AI Act - Regulation (EU) 2024/1689

13 Art. 50.4 of the AI Act

14 Art. 35(1)(k) of the Digital Services Act

15 Fenty v. Arcadia Group [2015] EWCA Civ 3

16 Fenty v. Arcadia Group [2015] EWCA Civ 3; Irvine v. Talksport [2003] EWCA Civ 423

17 Irvine v. Talksport Ltd [2002] EWHC 367 (Ch)

18 Sim v. H. J. Heinz Co [1959] 1 W.L.R. 313

19 Article 1019 of the Civil Code
20 Article 1023 of the Civil Code
21 s22 Act on the Protection of Copyright in Works of Art and Photographs (KunstUrhG or KUG)
22 by Sections 22 KUG
23 through a combination of Art. 2 I and Art. 1 I of the constitution
24 e.g., section 23 German Copyright Act (UrhG), CDPA '88
25 S30A CDPA '88 and Art. 5(3)(k) of the Copyright Directive (2001/29/EC), s. 51a German Copyright Act
26 S107 Copyright Act
27 U.S. Copyright Office, Copyright and Artificial Intelligence, Part 3: Generative AI Training (Pre-Publication Version, May 2025)
28 Copyright Law Article 24
29 s 73 German Copyright Act
30 S80 CDPA '88, S14 of the German Copyright Act (if this is likely to jeopardize his legitimate intellectual or personal interests in the work)
31 S84 CDPA '88, Clark v. Associated Newspaper [1998] 1 W.L.R. 1558
32 R 50/2024-2, Johannes Hendricus Maria Smit
33 S10 UK Trade Marks Act 1994; Art. 10 Trade Marks Directive (EU) 2015/2436, China Trademark Law Article 48, US Lanham Act
34 Clark v. Associated Newspaper [1998] 1 W.L.R. 1558
35 Federal Trade Commission Act
36 Anti-Unfair Competition Law Article 6
37 Act Against Unfair Competition (UWG)
38 Rule 3.1 of the CAP Code
39 SB 1571
40 HB 1133
41 Advertising Law Article 4
42 Anti-Unfair Competition Law Article 8
43 Art. 4 No. 1 GDPR, personal data is all information relating to an identified or identifiable natural person
44 Art 4.2 GDPR, UK GDPR, Chinese Civil Code and the Personal Information Protection Law
45 Art. 6 (1) Sentence 1 GDPR/DSGVO
46 e.g., Illinois Biometric Information Privacy Act (BIPA), the Washington My Health My Data Act, and the Texas Capture of Use of Biometric Identifier Act. There are 20 US state comprehensive privacy laws in effect or coming into

effect through January 2026 that grant those states' residents' rights regarding their personal information.

47 Section 42 (2) No. 1 of the Federal Data Protection Act (BDSG)

48 Defamation Act 2013

49 Civil reputation or criminal defamation

50 § 186 StGB [German Criminal Code] and § 187 StGB intentional defamation

51 § 263 StGB

52 Article 266 of Criminal Law

53 Protection of Harassment Act 1997

54 The Human Rights Act 1988

55 The case is likely to be stronger if there are specific factors present such as children (*Murray v. Big Pictures (UK) Ltd* [2008] EWCA Civ 446) or a private fancy dress party (*Mosley v. News Group Newspapers* [2008] EWHC 1777 (QB). Simple photos, e.g., on a public beach may prove to be more difficult (e.g., *Stoute v. News Group Newspapers* [2023] EWCA Civ 523).

56 § 826

57 § 164 I StGB

58 § 185 StGB

59 § 201a StGB

60 Criminal Law

61 [Financial Times article](#)

62 Section 230 of the Communications Decency Act 1996 (CDA)

63 Article 12–14 E-Commerce Directive (200/31)

64 Art. 16, 20–22 of the Digital Services Act; Article 9 of Provisions on the Governance of the Internet Information Content Ecosystem

65 As a new section 201b of the German Criminal Code

66 2025 annual session of the NPC

Related capabilities

Artificial intelligence

Technology

SUBSCRIBE

Interested in this content?

Sign up to receive alerts from the A&O Shearman on technology blog.

SIGN UP →

Register or update your preferences

