UNFAIR COMMERCIAL PRACTICES IN DIGITAL AGE[1]

Jana Strémy[2]

Abstract: The spread of digital technologies creates several risk vectors for traders. In this article, the author addresses the issue of unfair commercial practices occurring in the digital space. One such practice is deepfake, which has a high potential to mislead consumers because it presents individuals as saying or doing things they never said or did, which can adversely affect consumers' economic decisions. Deepfakes can create highly convincing manipulated audio-visual content that may falsely portray products, services, or even the identity of the trader. Such fabricated material can spread quickly across online platforms, increasing the likelihood that consumers will rely on misleading or entirely false claims when making purchasing decisions.The situation is particularly alarming for traders that use digital marketing tools, as legal liability is a major issue, especially for consumer-oriented content. Using standard methods in social sciences, the author identify a correlation between artificial intelligence technologies and unfair practices in order to assess the adequacy of legal regulation.

Key words: unfair commercial practices, artificial intelligence, deepfake, consumer, digital technologies, legal liability.

Introduction

In this new AI era, where the ability of machine to replicate the complexity of human is no more a fragment of science fiction but it is becoming reality day after day. Digi transformation brings entrepreneurs (traders) more possibilities of interaction with consumers. Traders engaged in the consumer facing platforms and e-commerce have used new technologies (from cookies to machine learning and AI) to track and predict consumer behaviour and influence his choice. According to some authors research shows that our human psychological characteristics can be accurately predicted from their digital footprints e.g. Facebook Likes or Tweets.[3] So far

[1] This contribution is funded by the EU NextGenerationEU through the Slovak Republic's Recovery and Resilience Plan as part of the Artificial Intelligence for Legal Professions (AILE) project No. 09I05-03-V02-00038.

[2] Faculty of Law, Comenius University in Bratislava

[3] MATZ, Sandra – KOSINSKI, Michal – NAVE,Gideon – STILLWELL, David: Psychological targeting as an effective approach to digital mass persuasion, In: Proc. Natl. Acad. Sci. U.S.A. 114 (48) 12714-12719,

doi: 10.46282/bpf.2025.19

however, national authorities stay *de facto* timid towards incorporating technologies in their daily work to monitor and detect wrongdoing. The fact that up to 84% of retailers already use artificial intelligence to execute and manage "shopping campaigns" illustrates the growing role of artificial intelligence in optimising business strategies.[4] According to a 2024 industry survey, 42% of retailers (and 64% of large retailers) already use some form of artificial intelligence. Nearly half of these retailers believe that generative AI will be a market differentiator.[5] AI accelerates and streamlines processes. However, it is also necessary to consider the other side of the coin: protecting the legitimate interests of consumers is challenging. AI technologies brings potentional risks of influencing consumers into making choices that do not serve their best interests[6] and it is transforming e-commerce and consumer interfaces, enabling merchants to interact with consumers in sophisticated ways. However, it is also raising issues such as manipulation, responsibility for content disseminated on the internet, the conflict between regulation and freedom of expression, the spread of alarmist news and the phenomenon of the 'liar's dividend'. It is particularly concerning that humans are still unreliable at identifying AI-generated content, often failing to recognise that they are interacting with a machine rather than a real person. This raises the issue of the challenges of consumer protection in the AI era. At first sight EU consumer law does not appear to be sufficiently clear or effective in tackling practices in the digital environment that undermine the effective enforcement of consumer rights, raising questions about the ability of the average or vulnerable consumer to make informed decisions about transactions. An essential aspect of consumers protection is *in natura* sufficient and effective legislation. Using analysis, comparison and synthesis, we tried to link the elements under scrutiny to observe the relationship between AI technologies and malpractices.

[online] 2017, [viewed 27 September 2025]. Available at: https://www.pnas.org/doi/full/10.1073/pnas.1710966114

[4] UNCTAD: Artificial Intelligence and Consumer Protection (Technical note produced within the framework of UNCTAD informal Working Group on Consumer Protection in e-commerce). [online]. 2024. [viewed 23 September 2025]. Available at: https://unctad.org/

[5] ZUMSTEIN, Darius – OEHNINGER, Fabian: Online Retailer Survey 2024 – Applications, Benefits, and Challenges of Artificial Intelligence in E-Commerce. [online]. 2024. [viewed 23 September 2025]. Available at: https://doi.org/10.21256/zhaw-2504

[6] TERRYN, Evelyne - MARQUEZ, Sylvia Martos: AI and Consumer Protection: An Introduction. In: SMUHA N.A., ed. The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence. Cambridge Law Handbooks. Cambridge University Press; [online]. 2025. [viewed 25 September 2025], p. 192-210 Available at: https://www.cambridge.org/core/books/cambridge-handbook-of-the-law-ethics-and-policy-of-artificial-intelligence/ai-and-consumerprotection/F5F0BBC5ABC0318DD902417C07482F6B#chapter

doi: 10.46282/bpf.2025.19

Malpractices of traders in digital enviroment

The use of artificial intelligence in the EU platform is regulated by the AI Act, formally adopted by The European Council on 21 May 2024 [7], which is the EU's first set of rules on AI. The AI Act was published in the Official Journal of the European Union on the 12 July 2024. However, it is not fully effective, with some exceptions[8] from 2 August 2026, and we can also call it the world's first comprehensive AI law. The AI Act provides us a „risk-based approach" classification for AI systems with variety of divergent requirements and obligations. Traders use artificial intelligence to improve ad targeting for consumers and ensure that marketing messages reach the right audience at the right time. AI also supports personalized shopping experiences through tools such as virtual shopping assistants that tailor product suggestions based on consumer preferences.[9] In addition, AI-powered chatbots are increasingly being used to communicate with consumers and provide exactly personalized advice. Despite the fact that these AI applications are useful, they also create fertile ground for abusive practices, which are not easily detectable for consumers. Many consumers are unaware that they are being manipulated by "dark patterns" .

In 2022, the European Commission and national consumer protection authorities across the EU conducted two sweeps and one of them was focused on using dark (deceptive) patterns on websites and apps. The Commission's 2022 dark patterns study based on showed that 97% of the most popular websites and apps used by EU consumers involved at least one dark pattern.[10] Due to the EU public consultation, 89% of consumers reported being perplexed by dark patterns in web or app design

[7] The AI Act was published in the Official Journal of the European Union on the 12 July 2024.

[8] E.g. on 2 nd February 2025 the ban of AI systems with unacceptable risks came info force. Codes of practice(9 months after entry into force) and Rules on general-purpose AI systems that need to comply with transparency requirements (12 months after the entry into force).

[9] See further: STRYCHARZ, Joanna – DUIVENVOORDE, Bram: The exploitation of vulnerability through personalised marketing communication: are consumers protected? In: Internet Policy Review vol. 10 (4). [online]. 2021. [viewed 25 September 2025] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991

https://policyreview.info/articles/analysis/exploitation-vulnerability-through-personalised-marketing-communication-are

[10](e.g. *Confirmshaming* i.e. passive-aggressive marketing strategy and emotional manipulation, *Nagging* i.e. asking repeatedly the same request, *Roach Motel* i.e. managing digital subscriptions like forced registrations and difficult cancellations, *Drip Pricing* i.e. hidden costs, *Urgency* i.e. deceptive fake countdown timers, Sneaking, i.e.. additive obligatory charges to a transaction at the final stage, etc.) See further: EUROPEAN COMMISSION: Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation. Final Report. [online]. 2022. [viewed 23 September 2025]. Available at: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en

doi: 10.46282/bpf.2025.19

(online interfaces) and 76% of consumers felt pushed to buy something.[11] In one of its reports[12], the OECD stated that, from the perspective of EU legislators, certain dark patterns can be addressed under the Unfair Commercial Practices Directive[13]. AI driven dark patterns as deceptive tactics used in consumers interfaces that exploit consumers psychology and behaviour can go even further in even more sophisticated ways than traditional dark patterns. The historic drafts of the AI Act[14] already emphasized that certain practices involving the misuse of technology for "*manipulative, exploitative, and social control practices*" are prohibited because they "*contradict... Union values*[15]*... and Union fundamental rights, including the right to non-discrimination, data protection and privacy, and the rights of the child.*" Some authors et al. rightly point out, "*pro futuro* use of AI systems can be difficult to predict, and it seems premature to permanently establish a list of prohibited AI practices."[16] Article 5(1)(a) AI Act contains prohibition of three alternative types of manipulative techniques. This article recognize subliminal techniques beyond a person's consciousness, purposefully manipulative techniques and deceptive techniques. In order for an artificial intelligence system to fall within the scope of Article 5(1)(a) of the Artificial Intelligence Act, it must use at least one of the following techniques. Subliminal techniques are "hidden" and eliminate a person's rational defense against manipulation (capable of influencing decisions without the person being aware of it), which evokes discussions about moral and ethical aspects due to the violation of an individual's autonomy, freedom of action, and free choice. In practice, these are stimuli delivered through audio, visual, or tactile media that are too brief or subtle for a person to notice like a visual, auditory and tactile subliminal messages, subvisual and subaudible cueing, capable of influencing emotions, attitudes sor behaviour of addressee. All above techniques are capable to distort human behaviour materially

[11] EUROPEAN COMMISSION: Commission Staff Working Document – Fitness Check. [online]. 2024. [viewed 23 September 2025]. Available at: https://commission.europa.eu/document/download/707d7404-78e5-4aef-acfa

[12] OECD: Dark Commercial Patterns. OECD Digital Economy Papers, No. 336. [online]. 2022. [viewed 24 September 2025], p. 20. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/10/dark-commercial-patterns_9f6169cd/44f5e846-en.pdf

[13] Art. 6 Misleading conduct, Art. 7 Misleading omissions or Art. 8-9 Aggressive practices

[14] See further: https://artificialintelligenceact.eu/documents/ i.e. AIA Committee Draft from 2 February 2024

[15] Values of respect for human dignity, freedom, equality, democracy and the rule of law.

[16] See also: SMUHA, Nathalie A. – RENGERS, Emma – HARKENS, Adam – LI, Wenlong – MACLAREN, James – PISELLI, Riccardo – YEUNG, Karen: How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act. [online]. 2021. [viewed 25 September 2025], p. 20. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991

doi: 10.46282/bpf.2025.19

and subvert free choice. *Pro futuro* subliminal techniques can be *"facilitated, for example, by machine-brain interfaces or virtual reality".* The EC guidelines specifies that *"AI can also extend to emerging machine-brain interfaces and advanced techniques*[17], as is stated in Recital 29. Although the ability to "read" a person's private thoughts using tools available to consumers is currently unattainable, it is necessary to discuss these nuances.

AI powered or deceptive innovation plaster?

Still growing number of companies are emphasising the integration of AI into their business models or the incorporation of AI into their products, as evidenced by the increasing prevalence of terminology such as "AI-driven" or "AI-powered" in their promotional materials. The term "AI washing" has been coined to denote the practice of asserting that products are powered by artificial intelligence even when they are not, or of exaggerating the capabilities of products that use artificial intelligence, thereby creating a misleading impression of innovation. The term "AI washing" bears a strong resemblance to the concept of "greenwashing,[18]" as far as it refers to the practice of companies exaggerating their environmental efforts.[19] The practice of AI washing, defined as the exaggeration or falsification of claims pertaining to the integration of AI in products or services with the intent to mislead consumers and investors, bears a notable similarity to the concept of "greenwashing," wherein environmental claims are made in a manner that is potentially misleading or deceptive. The following are examples of typical forms of AI: The term 'AI-powered' is often used to describe systems that utilise basic algorithms and automation, or human operators who masquerade as 'AI'. The exaggeration of the capabilities or functionality of the AI employed in a given product or service constitutes a significant aspect of the progress. There are known cases of misuse of artificial intelligence, for example in the field of investment in the US, where the US Securities and Exchange Commission accused two investment advisors of making false and misleading claims

[17] E.g. lucid dreaming through technology such as masks for sleeping or smartwatches connected to smartphones or machine-brain interfaces that permit users to play a game with headgear that detects brain activity

[18] See further: STRÉMY, Jana – ZLOCHA, Ľubomír: Unfair Competition or the Fine Line Between Green Marketing and Greenwashing. In: Adamová, Z. *Nové technológie, internet a duševné vlastníctvo.* 1. vyd. Trnava: Trnavská univerzita v Trnave, Typi Universitatis Tyrnaviensis, 2024, p. 87–99. ISBN 978-80-568-0709-5. [online]

[19] See further: EPERIESI-BECK, E.: Digitale Souveränität bei IT-Sicherheitslösungen endlich ernst nehmen. [online]. 2023. [viewed 12 September 2025]. Available at: https://www.security-insider.de/greenwashing-ai-washing-souveraenitaets-washing-digitale-souveraenitaet-datenschutz-a-9041e42caacf8977a7648ef0174edb77/

doi: 10.46282/bpf.2025.19

about the use of artificial intelligence to attract investors – financial consumers.[20] Further e.g. in the UK, the Advertising Standards Authority criticized an advertisement for an application that can be used to edit images allegedly using artificial intelligence as misleading.[21] In the retail sector In 2024, we can point to the widely publicized case of Amazon's "Just Walk Out" technology.[22] In the field of technology, some companies claim that their products are "powered by artificial intelligence," when in fact they do not use artificial intelligence or machine learning, but only conventional algorithms. The advertisement exaggerates the application's performance.[23] In our circumstances, it would be possible to punish conduct referred to as AI washing under unfair competition law, specifically Section 44 (1) of the Commercial Code.

Deepfake as a threat to virtual reality?

Although the definition of subliminal techniques in the AI Act seems extensive at first glance, its rationale focused on intent and degree of harm does not provide a comprehensive picture of how deepfake technology can manipulate consumers beyond conscious perception, cause deepfakes are explicitly created to reflect, but also distort, an individual's beliefs. As we have already mentioned, aspects of unreality in synthetic content are not easily recognizable to the human eye, and the role of artificial intelligence techniques (from the use of algorithms to disinformation) is to individually approximate replicated reality in synthetic content. In connection with technical solutions used by providers of artificial intelligence (AI) systems, entities deploying AI to generate or manipulate image, audio, or video content are required to clearly label such content as "deep fake." The AI Act partially overlooks this nuance, as evidenced by the relatively weak classification between limited-risk systems and completely prohibited practices. Of course, the risks emerging at present can only be observed step by step, but we should be aware of fact that deepfake technologies are not limited to one type or category of risk, but it would

[20] SEC: Charges Two Investment Advisers with Making False and Misleading Statements About Their Use of Artificial Intelligence. [online]. 2024. [viewed 24 September 2025]. Available at: https://www.sec.gov/newsroom/press-releases/2024-36

[21] ASA: Disclosure of AI in Advertising: Striking the Balance Between Creativity and Responsibility. [online]. 2023. [viewed 24 September 2025]. Available at: https://www.asa.org.uk/news/disclosure-of-ai-in-advertising-striking-the-balance-between-creativity-and-responsibility.html

[22] WOOLLACOTT, Emma: What is 'AI washing' and Why is it a Problem? [online]. 2024. Available at: https://www.bbc.com/news/articles/c9xx81228930

[23] E.g. In Slovakia the systém Pytagoras is presented as an intelligent online tool that helps brokers and financial advisors to efficiently manage administration, process contracts, and provide top-quality advice to clients, however, its background remains vague.

doi: 10.46282/bpf.2025.19

rather be a combination of „cascading effect at many different levels."[24] *Ad primum*, deepfakes targeting individuals often manifest themselves at the individual level. *Ad secundum*, they can cause harm to a particular group or organization. *Ad tertiam*, the cumulative effect of deepfakes can cause serious harm at the societal level. [25] Currently the most attention is dedicated to generative AI, which has been identified as a transformative force with the potential to significantly impact various industries and society as a whole.[26] To illustrate this point, consider the potential for deepfakes in advertising to mislead consumers, the exploitation of vulnerabilities by AI-generated personalised marketing, and the deceptive advice provided by B2C chatbots. This is primarily due to its ability to stimulate innovation, enhance individual autonomy, and augment productivity. However, one of the drawbacks of adopting this technology is that it is becoming increasingly difficult to distinguish human-generated content from synthetic content created by AI. This could potentially enable illegal and harmful conduct.[27]. If AI have capacity simulate different aspects of human intelligence (critically learning and decision making), then it could be argued that such capabilities would render AI applicable in circumstances where human discernment is required.

It is imperative to comprehend the significance, origins and scope of AI in order to understand its impact on consumers. Despite the majority of providers of generative artificial intelligence declaring that this technology should not be used for fraudulent purposes, the reality is quite different. For instance, fraudsters have started to utilise large language models to generate convincing phishing messages that are free of spelling and grammatical errors. Such errors have typically helped consumers identify scams in the past. Additionally, there have been instances of AI-generated deepfake audio being used to bypass voice recognition security systems on bank

[24] HUIJSTEE, Mariëtte van – BOHEEMEN, Pier van – DAS, Djurre – NIERLING, Linda – JAHNEL, Jutta Jahnel – KARABOGA, Murat – FATUN, Martin – KOOL, Linda – GERRITSEN, Joost: Tackling Deepfakes in European Policy. [online]. 2021. [viewed 25 September 2025]. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf

[25] Ibid. p.4-5.

[26] Generative AI has the potential to enable companies to automatically generate advertising copy and images, which could result in significant cost reductions. It has also the potential to enhance and automate personalised marketing, thereby enabling companies to deliver the appropriate persuasive message at the optimal time to each potential customer. These technologies offer potential advantages but also bear risks for consumers. See further: DUIVENVOORDE, Bram: Generative AI and the future of marketing: A consumer protection perspective In: Computer Law & Security Review, vol. 57, [online]. 2025. [viewed 25 September 2025]. Available at: https://www.sciencedirect.com/science/article/pii/S2212473X25000148)

[27] TAMBIAMA, Madiega: Generative AI and Watermarking. [online]. 2023. [viewed 10 September 2025]. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/757583/EPRS_BRI(2023)757583_EN.pdf

accounts. This demonstrates the potential of voice cloning to undermine biometric security systems and enable fraud. The potential for deepfakes to be used with alarming effectiveness in the context of consumer fraud has been well documented. Similarly, AI-generated text has been shown to be equally effective in the dissemination of misleading information and the influence of consumer decisions.

This article was also inspired by a case involving one of Slovakia's largest banks, Slovenská sporiteľňa, which is a paradigmatic example of victim of deepfake fraud in a business environment and in B2C relations. The corpus delicti consisted of deepfake videos appearing on YouTube and social networks in which the then CEO of the bank, Mr. P. Krutil, allegedly addressed viewers with an offer to invest through a new application that promised high and guaranteed returns. These videos were created with the intention of influencing financial consumers to make a business decision that they would not otherwise have made, i.e. investing funds in a fraudulent investment platform, with the attackers relying on the credibility that the bank and its senior representative had built up over many years of operating on the Slovak market. Such abuse of a person with the aim of misusing the credibility of an individual or institution is called „spoofing". Spoofing is a type of cyberattack that seriously threatens people's security and privacy. It occurs when an attacker pretends to be someone else—usually a trusted person or institution. Spoofing can take several forms: deepfake audio or video, where the likeness or voice of a well-known and trusted person is used to appear authentic (as was the case in the example mentioned earlier in this article); telephone spoofing, where the attacker calls from a number very similar to that of a bank or other institution, giving the victim the impression that it is an official call and prompting them to answer; or email and website spoofing, where fake emails or websites appear official at first glance. Therefore, spoofing is not only about misusing someone's image or voice in digital content, but more broadly about a false identity intended to deceive and exploit the victim's trust. The bank responded in kind with public warnings and alerts about the fake content of the videos, urging the public not to respond to such offers. There are several details that can help identify deepfakes, such as unusual lip movements, mismatches between sound and image, unnatural voices, or strange eye movements. Despite repeated warnings from the bank, the videos unfortunately remained active on YouTube, which pointed to the platform's inadequate response in detecting and blocking fraudulent content. In this regard, we also encounter the concept of hosting defense as defined in the Digital Services Act (DSA). Article 6 of Digital Services Act (DSA) has replaced the original eCommerce Directive's hosting defence in Article 14, but the core principle remains: a provider is exempt from liability for user-uploaded illegal content unless they possess knowledge of its

doi: 10.46282/bpf.2025.19

unlawful nature and fail to act. [28] It is important to note that Article 6 of the Digital Services Act requires platforms, upon obtaining such knowledge or information (about the harmful nature of content), to acts expeditiously to remove or disable access to illegal content. In this regard, it is also necessary to address the interpretation of "acts expeditiously." Although the interpretation of the term "illegal content" means any information which is not in compliance with Union law or the law of a Member State concerned is known, the interpretation of the phrase "acts expeditiously" remains vague and apparently subject to *ad hoc* assessment of circumstances. We suppose that it will be a matter of acting quickly and efficiently, or in a prompt manner, without undue delay. The impacts of this incident are, in fact, multidimensional. First and foremost, there is a direct risk to potential victims of deepfake fraud (financial consumers).[29] On another level, it is necessary to perceive the threat and damage to the goodwil of the trader, i.e. the bank, as well as the disruption of public confidence in its management. We can conclude that cyber attacks are also evolving from, say, widespread (general) fraud to sophisticated and targeted attacks. The misuse of the identity of the bank's executive director was therefore not accidental, with the aim of abusing trust in the authority and credibility of the person. This is a relatively new form of attack on the "digital identity" of a trader and shows that traditional security measures aimed at protecting networks and data are no longer sufficient today. According to the above, protection is now also required for the digital footprints and images of key figures, which are easily accessible on social networks. The incident at SLSP thus signals that in the future, one of the main targets of cybercriminals may be the direct manipulation of identity for financial gain and market destabilization.[30]

The dissemination of deepfake videos on social media platforms is a prevalent phenomenon, frequently characterised by malicious intentions[31]. Although in the

[28] Although the European Digital Services Act, which came into force in 2024, complements the AI Act in this regard by imposing more extensive obligations on online platforms. Its purpose is to combat illegal and harmful activities, including the spread of disinformation. Large online platforms are subject to stricter controls and must implement effective mechanisms for reporting and removing illegal content, including harmful deepfakes.

[29] TA3: Deepfake Can Cost You Thousands of Euros. SLSP Warns Against Fraudsters Who Misuse the Name of the Bank and the Media. [online]. [viewed 24 September 2025]. Available at: https://www.ta3.com/clanok/1005557/deepfake-vas-moze-pripravit-o-tisice-slsp-varuje-pred-podvodnikmi-ktori-zneuzivaju-meno-banky-aj-medii

[30] KPMG International: Deepfake Threats to Companies. [online]. 2025. [viewed 10 September 2025]. Available at: https://kpmg.com/xx/en/our-insights/risk-and-regulation/deepfake-threats.html

[31] Current examples of which have been shown across the encrypted messaging platform Telegram to spread propaganda around the Russian invasion of Ukraine. See further: GRIFFITHS, John: Deepfake Influencers: The Future of Fashion Advertising? [online]. 2022. [viewed 20 September 2025]. Available at: https://foundationagency.co.uk/blog/deepfake-influencers-the-future-of-fashion-advertising/

case of Slovenská sporiteľňa we can talk about i.e. deepfake spoofing [32] entails the utilisation of artificial intelligence (AI) to generate synthetic videos, images, or audio, which are designed to impersonate trusted individuals with a high degree of authenticity, thereby deceiving victims into divulging sensitive information or transferring funds. This term is defined in Article 3(60) of Regulation (EU) No. 2024/1689 of the European Parliament and of the Council (hereinafter also referred to as "AI Regulation"). This term is defined in Article 3(60) of Regulation (EU) No. 2024/1689 of the European Parliament and of the Council (hereinafter also referred to as the "AI Act") as content created or manipulated using AI that resembles existing persons, objects, places, entities, or events and may falsely appear to be authentic or true to a human being. Under this regulation, consumers must be clearly and conspicuously informed that the content has been created by artificial intelligence—for example, with labels such as "AI generated" or "made by AI." The AI Act also takes into account freedom of expression, artistic creation, and satire. In cases where deep fakes are part of artistic, creative, or satirical content, the transparency obligation is limited to disclosing the existence of such content in an appropriate manner that does not interfere with the experience of the work, its normal use, or its quality.[33] However, the question of what can be considered "appropriate" labeling is a matter of debate. One example was an AI model created by Seraphinne Vallora for the August 2025 issue of Vogue magazine, which was used in an advertisement for the Guess brand. Although Vogue labeled the content "produced by Seraphinne Vallora on AI" in accordance with Section 50(4) of the AI Act, consumers criticized the label as being too small and potentially misleading. Conversely, Vogue argued that a more prominent label would detract from the artistic nature of the magazine.

Another area where deep fakes are controversial is the use of famous people's faces in humorous, satirical, or other content without their consent. Such content can give the impression that the person depicted by AI is real, which can damage their reputation or lead to other illegal manipulations. Deep fakes are not only a problem in terms of potentially misleading consumers. Their use often also infringes on individuals' personal rights—for example, when an individual's image or voice is used without their consent. In such cases, Regulation No. 2016/679 (GDPR) also applies, as the face and voice can be considered biometric data. If a deep fake damages a person's reputation, there are legal tools available for defense – from personality

[32] Spoofing is cybercriminal masquerading as a trusted entity or device to deceive the user into performing an action that is beneficial to the hacker – and detrimental to the user. The act of concealing one's true identity by means of disguising or misrepresenting oneself is referred to as spoofing.

[33] REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL: Artificial Intelligence Act. Article 50, paragraph 4. [online]. [viewed 27 September 2025]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

protection under the Civil Code [34] to criminal consequences. Furthermore, if deep fakes are used in a commercial or public context without clear labeling indicating that the content is AI-generated, this may constitute a violation of the transparency obligations under the AI Act. Under Article 99(4)(g) of the AI Act, the competent authority may impose an administrative fine of up to 15,000,000 € or, if the offender is an undertaking, up to 3% of its total worldwide annual turnover for the previous financial year. The penalty is determined based on whichever amount is higher. The issue of deep fakes needs to be viewed in a broader context. In the United States, the Take It Down Act was passed on May 19, 2025, representing a major step forward in the regulation of AI-generated deep fakes.[35] The legislation in question also criminalises the publication of illegal intimate images without the consent of the person concerned, including those created using artificial intelligence. The legislation imposes an obligation on online platforms to remove such content within 48 hours of notification and introduces penalties of up to three years' imprisonment for offenders.[36] Another legislative step is the Deepfakes Accountability Act, which aims to protect national security from threats associated with deepfake technology and provides legal protection to victims harmed by the use of deepfake content.[37] This law should bring more transparency to the use of deepfake technology and also establishes legitimate remedies for victims. Beyond legal issues, deepfakes also pose a significant moral and social problem. AI-generated models often depict unattainable ideals of beauty that people naturally compare themselves to, which can lead to lower self-esteem and efforts to achieve a perfect appearance.[38] The Dove brand's 2024 advertising campaign also drew attention to the prejudices associated with artificial intelligence.[39] Despite the recent surge in attention to the issue of deep

[34] Act No. 40/1964 Coll., the Civil Code, (Občiansky zákonník). Sections 11 to 16.

[35] CONGRESS.GOV: S. 146 – Take it down Act. [online]. [viewed 28 September 2025]. Avaible at: https://www.congress.gov/bill/119th-congress/senate-bill/146

[36] CONGRESS.GOV: S.146 – Take it down Act., Article 60 paragraph 3. [online]. [viewed 28 September 2025]. Avaible at: https://www.congress.gov/bill/119th-congress/senate-bill/146/text

[37] CONGRESS.GOV: H.R. 5586 - Deepfakes Accountability Act. [online]. [viewed 28 Septemeber 2025]. Avaible at: https://www.congress.gov/bill/118th-congress/house-bill/5586/text

[38] Compare: Burkell, J. and Gosse Ch. note that deepfake technology, while "not inherently problematic," is rooted in social and cultural attitudes that can reinforce harmful consequences, such as exposing women to an increased risk of objectification and intimidation. BURKELL, Jacqeulyn – GOSSE, Chandell : Nothing new here: Emphasizing the social and cultural context of deepfakes, In: First Monday 24(12), [online] 2019, [viewed 25 September 2025]. Available at: https://firstmonday.org/ojs/index.php/fm/article/view/10287

[39] There, the image generator was asked to create "the most beautiful woman in the world." However, the results were almost identical figures—young, slim, with pale skin, light hair, and blue eyes. The images created in this way bore a striking resemblance to the visuals of the Guess AI model and reopened the debate about the stereotypes that artificial intelligence reproduces. BBC: Does this look

doi: 10.46282/bpf.2025.19

fakes and the gradual expansion of legislation, existing regulations are not yet deemed adequate to comprehensively address the risks, moral and ethical issues associated with this technology.

Application and limits of Deepfakes in current slovak legislation

Although Slovak law does not contain specific provisions on deepfakes, it provides a range of legal instruments that can be used to address such cases. However, it is necessary to take into account the fact that the effectiveness of these instruments may be limited in the digital environment. We can conclude that this is a fragmented and reactive system of legal protection[40]. Article 19(1) of the Constitution of the Slovak Republic guarantees the right of every individual to preserve their human dignity, personal honour and good reputation, as well as the protection of their name. In our country, the right to the protection of a natural person's personality is regulated by the provisions of § 11 et seq. of Act No. 40/1964 Coll. of the Civil Code. These provisions enshrine a group of absolute subjective rights that apply to everyone and are not subject to a statute of limitations. Protection of the personality includes name, honour, dignity and privacy, as well as likeness and voice. Therefore, the unauthorised use of the image and voice of the CEO of SLSP in a deepfake video constitutes a direct infringement of his personality rights. The right to one's image arises at the moment it is captured, including digital recordings. In the event of unauthorised infringement, the injured party may seek judicial protection by filing an action for injunctive relief, requesting that the perpetrator refrain from further infringements. In the case of deepfake content, this would mean requesting the removal of videos. The court may also award moral satisfaction (e.g. an apology) or, in cases of significant reduction in dignity and respectability in society, monetary compensation if the infringement has caused non-pecuniary damage. Although these provisions provide a legal basis for prosecuting deepfakes, they are reactive and dependent on the initiative of the injured party. They also face practical obstacles. In practice, identifying a perpetrator operating anonymously from another jurisdiction can be difficult, and the time limits for legal proceedings are insufficient given how quickly disinformation spreads on the internet. In this context, it is also necessary to refer to Section 19b(2) and (3) of the Civil Code, according to which a legal entity is entitled to certain protection in the event of an unjustified interference with its reputation. In accordance with the aforementioned provision, in the event of interference with the reputation of a legal entity (goodwill), it is possible to seek a

like a real woman? AI model in Vogue raises concerns about beauty standards. [published on 27 July 2025]. [online]. [viewed at 27 September 2025]. Avaible at: https://www.bbc.com/news/articles/cgeqeo84nn4o

[40] inconsistent, and respond only after a problem has occurred, rather than proactively preventing it

doi: 10.46282/bpf.2025.19

court order requiring the third party to refrain from interfering with the reputation, to remedy the defective situation, and to provide adequate satisfaction, which may also be claimed in monetary terms.

It is imperative to distinguish between such satisfaction and compensation for damages, as these are two discrete entities. Consequently, in addition to non-material damage, unauthorised interference with the reputation of a legal entity may also constitute damage, for which compensation may be sought on the basis of Section 420 of the Civil Code. We could also discuss the factual basis of unfair competition (e.g., misleading advertising promising guaranteed and high returns on fictitious investment platforms, which abused SLSP bank, could be classified as unfair competition together with parasitism).

Conclusion

In the era of artificial intelligence, it may sometimes seem that the only compass that helps us navigate the blurred lines between the real and the artificial is still our human discrement and in other cases, there is more or less effective legislation. In this article, we have focused on the problem of unfair practices by traders - retailers when using artificial intelligence technologies. The advent of artificial intelligence has a profound impact on the consumer experience, both online and offline. While we should evaluate sufficiency and efficiency of legislation therefore, the response to this question is not straightforward. When using artificial intelligence to generate advertisements, virtual influencers, or another commercial content, the content should include information such as "created by artificial intelligence" or "virtual character," especially in the case of consumer-oriented content. Transparency in the B2C sector is essential. Eliminating unfair practices such as dark patterns, AI washing, or deepfakes with fraudulent or malicious intent powered by artificial intelligence requires a comprehensive approach that involves consumers, developers, and at least regulators. The present legal framework in Slovakia is characterised by its fragmentation and a greater emphasis on reactivity in comparison to proactivity. It is to be hoped that the European legislator will provide greater clarity on the matter by the adoption and enforcement of the AI Act and the imminent Digital Fairness Act, the proposal of which is expected by mid-2026 and will introduce rules to prevent behavioural profiling, dark patterns, and AI-driven manipulative tactics.

Bibliography

1. ASA: Disclosure of AI in Advertising: Striking the Balance Between Creativity and Responsibility. [online]. 2023. [viewed 27 September 2025]. Available at: https://www.asa.org.uk/news/disclosure-of-ai-in-advertising-striking-the-balance-between-creativity-and-responsibility.html

doi: 10.46282/bpf.2025.19

2. BURKELL, Jacqeulyn – GOSSE, Chandell : Nothing new here: Emphasizing the social and cultural context of deepfakes, In: First Monday 24(12), [online] 2019, [viewed 25 September 2025]. Available at: https://firstmonday.org/ojs/index.php/fm/article/view/10287
3. CONGRESS.GOV: H.R. 5586 – Deepfakes Accountability Act. [online]. [viewed 28 September 2025]. Available at: https://www.congress.gov/bill/118th-congress/house-bill/5586/text
4. CONGRESS.GOV: S. 146 – Take it down Act. [online]. [viewed 28 September 2025]. Available at: https://www.congress.gov/bill/119th-congress/senate-bill/146
5. DUIVENVOORDE, Bram: Generative AI and the future of marketing: A consumer protection perspective In: Computer Law & Security Review, vol. 57, [online]. 2025. [viewed 25 September 2025]. Available at:https://www.sciencedirect.com/science/article/pii/S2212473X25000148)
6. EPERIESI-BECK, E.: Digitale Souveränität bei IT-Sicherheitslösungen endlich ernst nehmen. [online]. 2023. [viewed 12 September 2025]. Available at: https://www.security-insider.de/greenwashing-ai-washing-souveraenitaets-washing-digitale-souveraenitaet-datenschutz-a-9041e42caacf8977a7648ef0174edb77
7. EUROPEAN COMMISSION: Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation. Final Report. [online]. 2022. [viewed 23 September 2025]. Available at: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1
8. EUROPEAN COMMISSION: Commission Staff Working Document – Fitness Check. [online]. 2024. [viewed 23 September 2025]. Available at: https://commission.europa.eu/document/download/707d7404-78e5-4aef-acfa
9. EU: Regulation (EU) 2024/1689 of the European Parliament and of the Council – Artificial Intelligence Act. Article 50, paragraph 4. [online]. [viewed 27 September 2025]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689
10. EU Artificial Intelligence Act: Historic Documents. [online]. [viewed 02 February 2024]. Available at: https://artificialintelligenceact.eu/documents/
11. GRIFFITHS, John: Deepfake Influencers: The Future of Fashion Advertising? [online]. 2022. [viewed 20 September 2025]. Available at: https://foundationagency.co.uk/blog/deepfake-influencers-the-future-of-fashion-advertising/
12. HUIJSTEE, Mariëtte van – BOHEEMEN, Pier van – DAS, Djurre – NIERLING, Linda – JAHNEL, Jutta Jahnel – KARABOGA, Murat – FATUN, Martin – KOOL, Linda – GERRITSEN, Joost: Tackling Deepfakes in European Policy. [online].

2021. [viewed 25 September 2025]. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf

13. KPMG International: Deepfake Threats to Companies. [online]. [viewed 25 September 2025]. Available at: https://kpmg.com/xx/en/our-insights/risk-and-regulation/deepfake-threats.html
14. MATZ, Sandra – KOSINSKI, Michal – NAVE,Gideon – STILLWELL, David: Psychological targeting as an effective approach to digital mass persuasion, In: Proc. Natl. Acad. Sci. U.S.A. 114 (48) 12714-12719, [online] 2017, [viewed 27 September 2025]. Available at: https://www.pnas.org/doi/full/10.1073/pnas.1710966114
15. OECD: Dark Commercial Patterns. OECD Digital Economy Papers, No. 336. [online]. 2022. [viewed 24 September 2025]. p. 20. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/10/dark-commercial-patterns_9f6169cd/44f5e846-en.pdf
16. SEC: Charges Two Investment Advisers with Making False and Misleading Statements About Their Use of Artificial Intelligence. [online]. 2024. [viewed 28 September 2025]. Available at: https://www.sec.gov/newsroom/press-releases/2024-36
17. SMUHA, Nathalie A. – RENGERS, Emma – HARKENS, Adam – LI, Wenlong – MACLAREN, James – PISELLI, Riccardo – YEUNG, Karen: How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act. [online]. 2021. [viewed 25 September 2025]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991
18. STRÉMY, Jana – ZLOCHA, Ľubomír: Unfair Competition or the Fine Line Between Green Marketing and Greenwashing. In: Adamová, Z. *Nové technológie, internet a duševné vlastníctvo.* Trnava: Trnavská univerzita v Trnave, 2024, p. 87–99. ISBN 978-80-568-0709-5. [online].
19. STRYCHARZ, Joanna – DUIVENVOORDE, Bram:The exploitation of vulnerability through personalised marketing communication: are consumers protected? In: *Internet Policy Review* vol. 10 (4). [online]. 2021. [viewed 25 September 2025] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991 https://policyreview.info/articles/analysis/exploitation-vulnerability-through-personalised-marketing-communication-are
20. TA3: Deepfake Can Cost You Thousands of Euros. SLSP Warns Against Fraudsters Who Misuse the Name of the Bank and the Media. [online]. [viewed 24 September 2025]. Available at:

doi: 10.46282/bpf.2025.19

https://www.ta3.com/clanok/1005557/deepfake-vas-moze-pripravit-o-tisice-slsp-varuje-pred-podvodnikmi-ktori-zneuzivaju-meno-banky-aj-medii

21. TAMBIAMA, Madiega: Generative AI and Watermarking. [online]. 2023. [viewed 10 September 2025]. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/757583/EPRS_BRI(2023)757583_EN.pdf
22. TERRYN, Evelyne - MARQUEZ, Sylvia Martos: AI and Consumer Protection: An Introduction. In: Smuha NA, ed. The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence. Cambridge Law Handbooks. Cambridge University Press; [online]. 202. [viewed 25 September 2025], p. 192-210 Available at: https://www.cambridge.org/core/books/cambridge-handbook-of-the-law-ethics-and-policy-of-artificial-intelligence/ai-and-consumerprotection/F5F0BBC5ABC0318DD902417C07482F6B#chapter
23. UNCTAD: Artificial Intelligence and Consumer Protection (Technical note produced within the framework of UNCTAD informal Working Group on Consumer Protection in e-commerce). [online]. 2024. [viewed 27 September 2025]. Available at: https://unctad.org/
24. WOOLLACOTT, Emma: What is 'AI washing' and Why is it a Problem? [online]. 2024. Available at: https://www.bbc.com/news/articles/c9xx81228930
25. ZUMSTEIN, Darius – OEHNINGER, Fabian: Online Retailer Survey 2024 – Applications, Benefits, and Challenges of Artificial Intelligence in E-Commerce. [online]. 2024. [viewed 23 September 2025]. Available at: https://doi.org/10.21256/zhaw-2504

Contact details

doc. JUDr. Jana Strémy, PhD.
jana.stremy@flaw.uniba.sk
Department of Commercial Law and Economic Law
Faculty of Law, Comenius University in Bratislava

doi: 10.46282/bpf.2025.19