

Using Artificial Intelligence to Manipulate Images, Video or Audio (Deep Fakes) and Georgian Criminal Law

Bachana Jishkariani

Professor, PhD

The University of Georgia

Abstract

The development process of modern technologies, especially so-called artificial intelligence, poses new challenges to national and international criminal justice systems, as such technologies, on the one hand, make it easier to solve many issues simply, but on the other hand, they also present us with problems, since artificial intelligence can be used to commit various types of acts that may significantly violate others' rights and intensively intrude into one's personal space. Such actions require appropriate legal assessment, including through the application of criminal law, so that legal development keeps pace with technological progress.

The purpose of this article is not to review the broad aspects of artificial intelligence-related issues. It is limited to the problems of so-called Deep Fake in a comparative legal context concerning Georgian, European, and German criminal law, to assess the challenges in Georgian criminal law against the background of international experience. For this purpose, issues from Georgian, German, and EU legislation are analyzed, such as the unauthorized distribution of artificially generated materials containing someone else's image, production and distribution of pornographic material containing images of minors or adults, etc.

The analysis of individual problems shows that Georgian criminal law, although fragmentarily responding to modern challenges through the interpretation of existing norms, is clearly not sufficient, and a number of issues remain unregulated, which actually implies the absence of punishment. While it is not the function of criminal law to criminalize all types of violations, when it comes to gross and particularly intensive violations of others' dignity, privacy, or personal autonomy, the application of criminal law becomes necessary.

Keywords: Artificial intelligence, deep fakes, criminal law.

Introduction

The development process of modern technologies, especially artificial intelligence, is continuous and has become an integral part of our daily lives. Even if we consider our smartphones, such programs are already integrated into them and are being intensively used for various purposes, be it for translating texts or processing images. While such technologies, on the one hand, make it easier for us to solve many issues effortlessly, on the other hand, they also present challenges, as artificial intelligence simultaneously simplifies the commission of various types of actions that may significantly violate others' rights and intensively intrude into their personal space.¹ Such actions require appropriate legal assessment, including the application of criminal law, so that legal development keeps pace with technological progress.

The purpose of this article is not to review the broad aspects of artificial intelligence-related issues, as this would take us too far, but rather we will limit ourselves to the problems of so-called Deep Fakes. Along with the doctrinal research method, a comparative legal research method will be used in relation to Georgian, European, and German criminal law to assess the challenges in Georgian criminal law

¹ For example, human dignity must be protected from various types of violations. Regarding the right to dignity, see in detail Phirtskhalashvili, A., in commentaries Loladze, B., Phirtskhalashvili, A., *Fundamental Rights*, 2023, "Forma", par. 261 ff.

against the background of international experience. The necessity of this is due to the fact that there are no relevant specific studies in Georgian criminal law. Specifically, it is interesting to access to what extent such actions are punishable under the current edition of our criminal law legislation, and if they are not punishable, then what new approaches should be adopted to fill this gap?

1. The Concept of Artificial Intelligence

Before analyzing specific problematic criminal law issues, let's first explore the concept of artificial intelligence to gain a clearer understanding of its essence. Finding a unified, precise definition for this concept is difficult due to its complexity. Even the name itself is subject to various interpretations.

Specifically, as we know, intelligence, according to the prevailing approach so far, is associated with human abilities.² Intelligence doesn't only mean the human brain's ability to process received information. It is much more and is connected to many other abilities such as intuition, creativity, self-consciousness, etc.³ Consequently, the term artificial intelligence in scientific literature is sometimes put in quotation marks,⁴ emphasizing that it is not identical to the classical understanding of human intelligence. Additionally, the word "artificial" indicates that it's not about intelligence stemming from the human mind, but rather machine-related intelligence.⁵

Taking a brief definition of artificial intelligence, it refers to machines' ability to model human behaviors using complex algorithms.⁶ Regarding artificial intelligence-related issues, a high-level expert working group⁷ under the EU aegis also developed a definition in 2019, which briefly states: Artificial intelligence systems are human-created Software or Hardware systems that process existing data based on set goals and make the best possible decisions. These systems also have the ability to evaluate their previous behaviors and adapt to new environments.⁸

Overall, artificial intelligence should be viewed more as a collective term unifying various informatics methods, encompassing different tools. Using these tools, the programmer, in turn, should create and assemble new programs to accomplish specific tasks.⁹

We might wonder why there is so much discussion about the definition, however, we shouldn't forget that this is unavoidable when addressing potential legal problems and introducing relevant regulations. Any legislative body first assesses potential risks and only then adopts corresponding laws.¹⁰ Without defining the issue, especially introducing criminal liability will conflict with the principle of legal certainty.

In terms of international influences, the EU regulation on artificial intelligence, adopted on June 13, 2024, which has already entered into force, is important.¹¹ The very first part of Article 3 of the regulation talks about the "system of artificial intelligence," however, this definition is not particularly narrowly formulated and refers to a mechanical system (so to speak, "machine") that can act somewhat autonomously based on specific objectives through making predictions, giving recommendations, or making decisions, which in turn can influence this system's physical or virtual environment.

² Waxnegger, K., „Künstliche Intelligenz und Strafrecht“, „Österreich“, 2024, p. 7.

³ Ibid. p. 7-8.

⁴ Cornelius, Kai, „Criminal Law Challenges of Artificial Intelligence“, in collection Jishkariani, B., Wassmer, M. (editors), Criminal Law and Human Rights, "World of Lawyers", 2024, p. 158.

⁵ Busche, D., „Einführung in die Rechtsfragen der künstlichen Intelligenz“, „Juristische Ausbildung“, 2023, p. 441.

⁶ Gunnar, G., in Weber, K. (Ed), Weber Kompakt, Rechtswörterbuch, „Beck“, 2024 (Künstliche Intelligenz).

⁷ <https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai> (l. s. 14.02.2025).

⁸ Hochrangige Expertengruppe für künstliche Intelligenz, Eine Definition der KI: Wichtigste Fähigkeiten und Wissenschaftsgebiete, p. 6.

⁹ Busche, D., „Einführung in die Rechtsfragen der künstlichen Intelligenz“, „Juristische Ausbildung“, 2023, p. 442.

¹⁰ Steege, H., „Haftung für Künstliche Intelligenz im Straßenverkehr“, „Straßenverkehrsrecht“, 2023, p. 10.

¹¹ Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz - ABl. L 2024/1689, 12.07.2024.

Such a broad definition might be considered justified, at least at this stage, since artificial intelligence systems are still in development. However, to address individual criminal law challenges, we will need to go into more detail for greater specificity. One such challenge related to artificial intelligence is the manipulation of images, videos, or audio.

2. What are Deep Fakes?

As already highlighted, the spread of artificial intelligence, which is now an irreversible process at this time, along with its many positive aspects, is also associated with significant risks.¹² One manifestation of this is, for example, the manipulation of others' photos, videos, or voice and presenting them realistically, which can then be used in various directions, whether as influencing elections or distributing pornographic material.

Artificial intelligence "learns" based on existing data, and consequently, a well-"trained" artificial intelligence can simulate even someone else's voice, making it difficult to distinguish from the real one.¹³ Such manipulations are so close to the real picture that they can be easily used to create disinformation and incorrect perceptions.¹⁴ We can compare this technology to existing editing, but the qualitative difference is much greater. With the help of artificial intelligence, it is possible to make manipulations that they can make a real person "say" words in a recording that appear very realistic in terms of sound and lip movement, when in reality, this person never actually said such a thing.¹⁵ Artificial intelligence uses sentences previously (in reality) said by a specific person, audio and video material to learn how to create new, imitated recordings.¹⁶ Additionally, artificial intelligence can even imitate specific people's behaviors and facial expressions, making it difficult to distinguish between reality and imitation.¹⁷

The issue of Deep Fakes has remained relevant since 2017, that is, since it first appeared in the media. Initially, it attracted attention through the imitation of politicians, however, such unauthorized imitations can have equally negative consequences for private individuals.¹⁸ For example, someone might use another person's voice to deceive others during a phone conversation or create pornographic material, etc.

Hence, it appears that Deep Fakes threatens not only universal legal goods (e.g., stability of the electoral process) but also individual legal goods (e.g., protection of others' property from fraudsters).¹⁹ Consequently, from a criminal law perspective, when implementing such manipulations, to effectively protect legal goods, we cannot limit ourselves to just one specific section of the Criminal Code.

Given the relevance of the issue, Deep Fakes has not been left out of the attention of the new EU regulation either. According to Article 3 (60) of the regulation, this is an image, video, or audio created or manipulated by artificial intelligence that resembles real people, objects, places, institutions, or events that might appear authentic to humans.²⁰

¹² See also Thiel, M., „Deepfakes“ – Sehen heißt glauben?“, „Zeitschrift für Rechtspolitik“, 2021, p. 202.

¹³ Lantwin, T., „Strafrechtliche Bekämpfung missbräuchlicher Deep Fakes“, „Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT“, 2020, p. 78.

¹⁴ Tilson, Luke B., Eichinger, D., „KI-generierte Deepfakes und ihre Gefahr für Kapitalmärkte“, „Zeitschrift für Bank und Kapitalmarktrecht“, 2024, p. 648.

¹⁵ Lantwin, T., „Strafrechtliche Bekämpfung missbräuchlicher Deep Fakes“, „Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT“, 2020, 78.

¹⁶ See also Cornelius, K., Criminal Law Challenges of Artificial Intelligence, in collection Jishkariani, B., Wassmer, M. (editors), „Criminal Law and Human Rights“, "World of Lawyers", 2024, p. 158.

¹⁷ See in detail Thiel, M., „Deepfakes“ – Sehen heißt glauben?“, „Zeitschrift für Rechtspolitik“, 2021, p. 203.

¹⁸ Rößling, F., Manipulierte Medien in AI Act, DS-GVO und allgemeinem Persönlichkeitsrecht, ZfDR 2024, 187.

¹⁹ Thiel, M., „Deepfakes“ – Sehen heißt glauben?“, „Zeitschrift für Digitalisierung und Recht“, 2021, p. 202.

²⁰ Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz - Abl. L 2024/1689, 12.07.2024.

3. Malicious Use of Deep Fakes

3.1. Production or Distribution of Deep Fake Pornographic Content Containing Images of Minors

Article 255 of the Criminal Code of Georgia addresses the illegal production or distribution of pornographic content or other materials. Although the first part of this provision has been declared void since May 1, 2023, based on the Constitutional Court of Georgia's decision²¹ - as the court believed that legislation does not define the concept of pornography, which causes ambiguity in the norm and therefore cannot be used as grounds for criminal prosecution - this does not apply to the entire norm. Actions related to minors remain punishable (Article 255, (3, and following parts of the Criminal Code))

The note to Article 255 of the Criminal Code explicitly states that pornographic content containing images of minors is any visual or audiovisual material created by any method. It can be even simulated or generated using computer technologies.²² Therefore, pornographic material containing images of minors created using artificial intelligence falls unproblematically under criminal liability. Although material created using artificial intelligence, simulated, featuring a non-real minor, does not harm one specific person, meaning we won't have one specific victim, this is irrelevant anyway, since Article 255 of the Criminal Code does not necessarily protect individual legal interests. Creating or distributing pornographic material containing images of minors is punishable because it poses a threat to minors in general and their normal development.²³ Therefore, since the criminal prohibition serves to protect adolescents, it is an abstract danger delict.²⁴

The following case requires broad interpretation of the norm: An adult establishes communication with a 17-year-old minor, records their voice, and later uses this minor's voice in a pornographic film where not the minor themselves is filmed, but rather an adult. The perpetrator (who does not appear to be a minor) will, through artificial intelligence, "overlay" the minor's voice onto someone else's image.

Article 255 (5) provides for criminal liability when dealing with pornography containing images of minors with prior knowledge. At first glance, audio cannot be considered an image, but according to the first paragraph of the note to Article 255, pornographic content containing images of minors also implies audiovisual material. Although the word "audiovisual" is not exactly synonymous with "audio" in a narrow sense, it implies more and includes audio as well. Therefore, in our case, punishing the perpetrator under Article 255(5) is possible.

Questions may arise about whether such cases need to be subject to criminal liability at all, but from the perspective of protected legal interests, using children's audio material is no less potentially harmful. In the era of artificial intelligence, manipulation of images and voices has become much simpler. Consequently, the above-discussed provisions of the Criminal Code require certain new interpretations in practice.

The same approach should apply to Articles 255¹ and 255² of the Criminal Code of Georgia. For example, if a person creates simulated pornographic material containing images of an adult using artificial intelligence and, let's consider, uses a minor to distribute it, this would constitute the elements of Article 255¹ of the Criminal Code of Georgia.

²¹ Decision of the Constitutional Court of Georgia #1/8/926, on the case of Giorgi Logua vs. Parliament of Georgia. <https://matsne.gov.ge/ka/document/view/5609438?publication=0#DOCUMENT:1>; (l. s. 18.02.2025).

²² This definition derives from the 2011 EU Directive on combating sexual exploitation of children and child pornography (ABl. L 335, 17.12.2011). See in detail Jishkariani, B., „European Criminal Law within the European Union, Tbilisi“, "World of Lawyers", par. 503 ff.

²³ Compare Eisele J., Duman, I., „Criminal Liability of Deepfake Pornography under Turkish and German Criminal Law“, 1 „Zeitschrift für Internationale Strafrechtswissenschaft“, 2025, p. 70-71.

²⁴ Zimmermann, F., in Satzger, H., Schluckebier, W., Werner, R. (Editors), „StGB Kommentar“, „Carl Heymanns Verlag“, 2024, § 184 Rn. 9.

3.2. Creation or distribution of Deep Fake pornographic or other material containing adult images

As indicated previously, the issue of criminal regulation of production or distribution of pornography containing adult images, based on the Constitutional Court's decision, remains unresolved and depends on future legislative changes. Until then, no one can be held criminally liable. For example, if a person uses their own video camera to make a pornographic short film with the consent of other adults (actors) and then distributes it, this would not be criminally punishable.

The fact that such an act is not a crime is not necessarily a significant challenge, as it is already difficult to justify what legal good is protected when producing or distributing voluntarily recorded pornographic material containing adult images, since no one is harmed or endangered by it.²⁵ It doesn't matter whether such material was created using artificial intelligence or with the participation of real people. However, beyond this example, we may encounter many challenges that extend far beyond the scope of pornography and are related to issues of human dignity, sexual integrity, or personal autonomy.

In consideration of the above discussed, stalking is thought-provoking as a crime against human rights and freedoms. The Georgian Criminal Code protects precisely the freedom of human will by introducing this composition in 2017 as Article 151¹. Protection from stalking is also related to protecting the victim's inner peace.²⁶ For comparison, a similar approach exists, for example, in German criminal law, which speaks about the freedom to arrange one's own life,²⁷ the victim's freedom of action,²⁸ etc.

Although Georgian criminal legislation previously recognized compositions of duress (Art. 150) and threats (Art. 151), which are also considered crimes against human rights and freedoms, these compositions could not handle actions characteristic of stalking in the modern sense.²⁹ While theoretically, it was possible to broadly interpret Article 150 of the Criminal Code of Georgia, coercion, and include stalking within it, overcoming decades of established court practice and transitioning to such broad interpretation would have been quite difficult. Additionally, from a theoretical perspective, it would become debatable whether certain actions would fall under the composition of duress.

To determine the punishability of stalking committed through Deep Fake manipulations, let's examine Article 151¹ (1), of the Georgian Criminal Code. It defines stalking as follows: illegal surveillance of a person, their family member or close relative personally or through a third party, or establishing unwanted communication via telephone, electronic or other means, or any other intentional action that is carried out systematically and causes psychological suffering to a person and/or creates reasonable fear of violence against the person or their family member or close relative or destruction of property, which forces the person to significantly change their way of life or creates a real need for such significant change.

Therefore, for punishability, first, the action must be carried out systematically, and also, such intensity of impact must be exerted on the victim that they at least consider changing their lifestyle. In other words, the victim must experience significant internal discomfort due to stalking by another person.³⁰

²⁵Although there is a discussion in Georgian legal literature about the protection of public morality - see Lekveishvili, M., Mamulashvili, G., Todua, N., Criminal Law Special Part (Book 1, Part Two), "Meridiani", 2023, p. 430 - however, this is a very general legal good and does not fit into modern criminal law approaches.

²⁶ Jishkariani, B., „Special Part of Criminal Law, Crimes Against the person“, "World of Lawyers", 2022, par. 1050.

²⁷ Valerius, N., in BeckOK StGB, v. Heintschel-Heinegg, B, Kudlich, H. (Editors), 64. Edition, „Beck“, 2025, § 238 Rn. 1.

²⁸ Heger., M., in Lackner, K., Kühl, K., Heger, M., „StGB“, „Beck“, 2023, § 238 Rn. 1; Eisele, J., in Schönke, A., Schröder, H., „Strafgesetzbuch“, „Beck“, 2019, § 238 Rn. 4.

²⁹ Jishkariani, B., „Stalking in Georgian Criminal Law“, in the collection Jishkariani, B., Wassmer, M. (editors), „Criminal Law and Human Rights“, Tbilisi, "Lawyers' World", 2023, p. 145.

³⁰ Jishkariani, B., Special Part of Criminal Law, „Crimes Against the person“, "World of Lawyers", 2022, par. 1070.

Considering the topic of the article, a pertinent question arises: can the distribution of Deep Fake pornographic material created using artificial intelligence be considered stalking? Let's consider the following example: A person, angry at their ex-spouse for refusing to reconcile, created a Deep Fake video using artificial intelligence where their ex-spouse supposedly participated in certain sexual acts. Then they uploaded this video to a social network. Because of this, the ex-spouse became deeply distressed and, feeling ashamed, completely deleted their social network accounts and reduced communication with acquaintances.

Upon initial observation, such action falls under the definition of stalking provided in Article 151¹ (1) of the Criminal Code of Georgia. Although the norm doesn't directly mention this specific form of action, it talks about any other action that creates the need for significant change in the victim's way of life. The ex-spouse's (victim's) deletion of social network accounts and reduction in communication with others clearly constitutes a significant change in lifestyle. Social contacts are a very important factor for any person. However, from a criminal law perspective, the absence of one important prerequisite provided by law - systematic nature of the action - will create a problem for punishability. Uploading a video once to the internet cannot be assessed as systematic action. Systematic nature implies repeated actions with certain frequency. Therefore, criminally, the victim is completely unprotected.

Instead of stalking, we might have considered violation of personal life under Article 157¹ of the Criminal Code of Georgia, as illegal distribution of someone's intimate pictures or video is a crime. However, in this case, the problem is that no real victim appears in the artificially generated video. Their personal life privacy, as the subject of the crime, doesn't exist at all - it's simply invented using algorithms. For comparison, German criminal law faces the same challenges in terms of stalking composition. Although specifically in paragraphs 6-8 of § 238 (1) of the German Criminal Code, it mentions (among others) the distribution of images that diminish a person in others' eyes, German legislation also requires repeated action for stalking to be punishable.³¹ German Criminal Code, in contrast to the Georgian one, recognizes such a criminal offense (§ 201a (2)) that concerns making a person's photo available (distributing) to third parties without permission. However, the main objective prerequisite of the crime is that this action must pose a significant threat to the person's reputation. Although this norm does not cover drawings and caricatures, this restriction does not extend to video editing,³² including the use of artificial intelligence. Distribution of Deep Fake pornography will indeed put a person in a particularly awkward position in the eyes of others.³³

Paragraph 201a (2) of the German Criminal Code only concerns distribution and not production. The creator of Deep Fake imagery, whether pornographic or other material, will not fall under this norm.³⁴ Criminal liability requires unauthorized transfer of such material to another person. There is ongoing discussion regarding the distribution of so-called links, through which the uploaded material can be viewed. In both legal doctrine and court practice, different approaches can be encountered on this matter.³⁵ If we look at the norm as a danger-generating offense, then sharing a link, even without opening it by a third party, already creates a serious threat to the victim's reputation. Consequently, such action should already be assessed as a completed crime.

³¹ Eisele J., Duman, I., „Criminal Liability of Deepfake Pornography under Turkish and German Criminal Law,“ 1 „Zeitschrift für Internationale Strafrechtswissenschaft“, 2025, p. 74-75.

³² Bosch, N., in Satzger, H., Schluckebier, W., Werner, R. (Editors), „StGB Kommentar“, „Carl Heymanns Verlag“, 2024, § 184 Rn. 9.

³³ Lantwin, T., „Strafrechtliche Bekämpfung missbräuchlicher Deep Fakes“, „Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT“, 2020, p. 79.

³⁴ Bosch, N., in Satzger, H., Schluckebier, W., Werner, R. (Editors), „StGB Kommentar“, „Carl Heymanns Verlag“, 2024, § 184 Rn. 18; Kumkar, L.K., Rapp, J.P., „Deepfakes, Eine Herausforderung für die Rechtsordnung“, „Zeitschrift für Digitalisierung und Recht“, 2022, p. 209.

³⁵ Heger, M., in Lackner, K., Kühl, K., Heger, M., „StGB“, „Beck“, 2023, § 201a Rn. 7; Bosch, N., in Satzger, H., Schluckebier, W., Werner, R. (Editors), „StGB Kommentar“, „Carl Heymanns Verlag“, § 184 Rn. 24.

Georgian criminal law does not recognize analogous provision to paragraph 201a of the German Criminal Code. Consequently, such actions remain unpunished, which, from a criminal law perspective, is unjustifiable. In fact, any person can, through simple technological manipulations using artificial intelligence, create intimate images of a specific person to damage their reputation and distribute them without facing any criminal repercussions. As a result, the victim's private life and dignity remain entirely unprotected.

Indeed, the legislator's aim should not be to criminalize as many actions as possible and apply criminal law expansively, however, cases involving particularly intensive actions that violate human dignity should not be left overlooked. The existing norms in the Criminal Code of Georgia (Articles 157, 157¹), from the perspective of protecting private life, do not cover aspects of the distribution of artificially generated material.³⁶

Under Georgian legislation, the creator and distributor of such Deep Fake material may be accountable under criminal law, for example, for extortion (Article 181). This would be the case when a person creates defamatory generated material using artificial intelligence and tries to obtain a certain amount from the victim by threatening to distribute this material. Although the victim is not actually depicted in the material at all, using their image in undesirable scenes through technology will pose significant challenges from a social perception standpoint. For qualifying the action as extortion, it is entirely sufficient to threaten to publicize or distribute any defamatory information.³⁷ Therefore, the perpetrator is held accountable for committing a crime against property rather than for such violation of human dignity that could destroy their reputation in the eyes of others.

3.3. Possible variants of committing other crimes using Deep Fake

Artificially generated materials containing someone else's image can also be used to commit such "classic" crimes as murder. The focus here is not on the direct malicious user of artificial intelligence, but on how the user provokes another person. For example, one person shows another person a Deep Fake video with the image of their spouse, as if they are cheating and meeting someone. Because of this, the angry husband, as the second person, will kill his wife. The video was so realistic that he didn't even doubt its authenticity. Regarding this case, determining the responsibility of the murderer is simple. He will be punished under Article 109 (k) of the Criminal Code (murder of a family member), but it is problematic to criminally prosecute the person who created the fake video.

We could have contemplated holding them accountable for complicity in crime as an instigator using Articles 24 and 25 of the Criminal Code, but merely showing someone a video is insufficient. Complicity is considered to be persuading someone to commit an intentional crime (Criminal Code Article 24 (2)). Persuasion requires undeniable intellectual contact between the perpetrator and the instigator.³⁸ Simply showing a video to someone does not reach the intensity of persuasion. Additionally, the proposal to commit a crime must be specific.³⁹ The fact that one person shares some information with another, and then, based on anger, this second person kills someone else, clearly does not fit the definition of instigation. Therefore, the author of the fake video cannot be punished at all. This is precisely why it is desirable to have a provision similar to paragraph 201a of the German Criminal Code in the special part of the Georgian Criminal Code, so that at least the victim's dignity and private life are protected in this particular case, and the distributor of the fake video can be punished.

³⁶ Dvalidze, I., in Dvalidze, I., Kharanauli, L., Tumanishvili, G., Tsikarishvili, K., „Crimes against Human Rights and Freedoms according to the Criminal Code of Georgia“, "Meridiani", 2019, 386 ff.

³⁷ Jishkariani, B., „Special Part of Criminal Law, Crimes against Property“, "World of Lawyers", par. 334-335.

³⁸ Mtchedlishvili-Hädrich, K., „Criminal Law, General Part, Individual Forms of Crime Manifestation“, "Meridiani", par. 424.

³⁹ Todua, N., in Group of authors, Todua, N., Ivanidze, M., Turava, M. (editors), „General Part of Criminal Law, Commentary, Volume 2“, „Kalmosani“, 2021, p. 390.

Concerning the use of artificial intelligence, Article 180 of the Criminal Code of Georgia - Fraud - is relevant in terms of deceiving others. The fraudster gains possession of another's property through deception. The victim, due to their own mistake, willingly transfers the item or property right to the offender because they believe the promise.⁴⁰ Although internet fraud is already widespread, unfortunately this process will become even easier with the use of Deep Fake content. The offender can more quickly create, for example, a clothing sales website and thereby gain access to potential buyers' funds who place orders. When a person directly takes possession of these funds themselves, they will be punished as the perpetrator under Article 180 of the Criminal Code of Georgia. But if they create such a site for another person without participating in subsequent processes, this will constitute complicity in fraud, specifically aiding.

Regarding fraud, the use of fake reviews on online store pages is also noteworthy. Specifically, this refers to supposedly positive reviews left by buyers about various products, when in reality, these products are of much lower quality. In practice, such reviews significantly influence the buyer's decision-making process.⁴¹ When a specific online store deliberately uses artificially created reviews that are not written by real people but generated by artificial intelligence to sell their products, this constitutes fraud (Criminal Code Article 180) or consumer deception (Criminal Code Article 219).

As a counter-argument to punishment, one might think that a large portion of internet users already know about the existence of fake reviews to some degree on online store pages and therefore they are taking a conscious risk, meaning they are not being deceived. But this approach would not be correct. No individual client specifically thinks they are being deceived.⁴² They only abstractly assume the existence of incorrect reviews on the online store site. When purchasing a product for themselves, they still act more on trust. If punishment were rejected, consumer property would largely remain unprotected, which would be misaligned with modern reality, since an increasing number of purchase transactions are conducted online, which would remain beyond criminal law regulation.

The issue of fake reviews should not be confused with product advertising where the properties are correctly presented, but artificial intelligence-created Fake videos with people involved in it and where these artificially created individuals emphasize certain product features to attract buyers. In this case, the buyer is not being misled. They are provided with correct information and their payment for purchasing a product will not be based on deception.

Fake reviews are also used to damage the image of competing companies. This can spread to many areas, from spreading Fake negative reviews of others' artworks to defaming cosmetic or other products. Such actions can have various motives. For example, simple revenge against others, bankrupting competitor companies, etc. The use of artificial intelligence enables the dissemination of significantly more convincing and harmful information about others' works or products.

Would such actions be subject to punishment under the Georgian Criminal Code? Generally, Georgian legislation does not recognize criminal punishment for defamation or insult for objective reasons. In a judicial system, in the process of establishing new democracy, there are serious risks of misuse of such provisions (for example, when a high-ranking official is accused of corruption and demands criminal punishment of others for defamation using their influence). With legislative changes in 2004, defamation was decriminalized. Drawing from this, it was regulated in the Georgian Law on "Freedom of Speech and Expression", which in turn automatically became subject to civil proceedings.⁴³ Therefore, Georgian legislation considers defamation, like several cases of protection of non-property

⁴⁰Jishkariani, B., „Special Part of Criminal Law, Crimes against Property“, "World of Lawyers", 2024, par. 270.

⁴¹ Heinelt, H., „Sind Fake-Bewertungen strafbar?“

Strafbarkeit fingierter Kundenbewertungen aus Sicht der Ersteller und der Betreiber von Bewertungsplattformen, „Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT“, 2022, p. 857.

⁴² Ibid, p. 858.

⁴³ Jorbenadze, S., „Defamation on Social Media and Means of Legal Protection in Georgian Court Practice“, in Jishkariani, B., Wassmer, M. (editors), „Criminal Law and Human Rights“, "World of Lawyers", 2023, p. 91.

rights, within private law and the only way to protect rights is through court appeals.⁴⁴ Accordingly, for reputational damage, the civil law path remains - claiming moral and property damages. In this case, it is the plaintiff's burden of proof whether they suffered property or non-property damage.⁴⁵

Besides the civil law path, Article 286² of the Georgian Criminal Code is thought-provoking, which concerns the creation of false computer data. The norm states that it is punishable to receive false official computer data by unauthorized insertion, deletion, modification or concealment of computer data with the purpose of presenting and/or using it as genuine/authentic data, as well as selling and/or using it. This article appeared in the Criminal Code as a result of changes implemented in 2021 and is quite broadly formulated, which is already problematic in terms of norm definition.

Despite the general content of the norm, it does not cover cases of damaging anti-advertisement of others' names or products that we discussed above. This is also supported by the explanatory note to the law, which nowhere mentions creating Fake images using artificial intelligence. The spirit of the changes implemented at the time was quite different and served to effectively protect others' property through the use of computer systems (e.g. computer fraud).⁴⁶

Additionally, in case of reinterpreting the norm to criminally punish anti-advertisement, it would create systemic contradiction within the Criminal Code of Georgia itself, because as we mentioned above, a legal-political decision was made to abolish the punishment of defamation. Accordingly, defamation through artificially falsified videos or other content cannot become a crime through broad interpretation of the norm. This would require appropriate legislative changes rather than simply changing court practice. Otherwise, we would get a strange picture - defamation through computer manipulations would be punishable based on Article 286², while using other methods would not be, which could not fit into the logic of unified criminal policy.

The use of artificial intelligence encompasses a broader spectrum of potential crimes than just human privacy, their intimate sphere, dignity, or even property. For example, Article 369¹ of the Criminal Code of Georgia concerns the falsification of evidence in criminal cases. Falsification is essentially the manipulation of evidence through which a person tries to influence the judicial process. Therefore, this norm protects not just one specific individual, but the interests of justice as a whole.⁴⁷ From this perspective, in cases where video evidence exists, Deep fake manipulation cannot be ruled out to alter the real picture shown in the recording. Additionally, video evidence might not exist at all, but could be created using artificial intelligence to mislead the investigation or court.

While it's true that technical methods and expertise will likely identify such falsified evidence, this is not pertinent to criminal liability. Prosecution under Article 369¹ does not necessitate the occurrence of any specific outcome (a crime without result).⁴⁸ The important thing is that the video manipulator acted with the intent to falsify evidence. Whether they ultimately achieved their goal of misleading justice is irrelevant. This approach equally applies not only to the falsification of evidence in criminal cases but also to civil or administrative cases (Criminal Code Article 369).

Another form of crime that poses a threat not only to individuals but to the entire state and society is terrorism. This paper will not discuss all terrorism-related provisions from Georgian legislation, but for the purposes of the article, in relation to artificial intelligence, we will discuss one of them - Article 330¹ of the Criminal Code of Georgia, public support for terrorist activities and/or terrorist organizations or public calls for terrorism. More specifically, it is punishable to publicly support terrorist activities and/or terrorist organizations orally, in writing, or through other means of expression if it creates a clear, direct, and substantial threat of terrorist activity. It is also punishable to publicly call for terrorist

⁴⁴ Ibid, p. 88.

⁴⁵ Ibid, p. 95.

⁴⁶ Explanatory Note to the Draft Law - <https://info.parliament.ge/file/1/BillReviewContent/268580> [L. s. 22.02.2025].

⁴⁷ Lekveishvili, M., Mamulashvili, G., Todua, N., „Criminal Law Special Part (Book 2)“, "Meridiani", 2020, p. 541.

⁴⁸ Ibid, p. 541.

activities orally, in writing, or through other means of expression, or to publicly disseminate information for carrying out terrorist activities, regardless of whether it contains a direct call to commit a crime, if it creates a clear, direct, and substantial threat of terrorist activity.

This article will cover the distribution of Deep fake materials (video, pictures, audio, etc.) created using artificial intelligence by a specific person, which is carried out to support terrorism. It doesn't matter whether this person will be directly depicted in the said material or will use another person's image for more effectiveness. To imagine a more specific example: a person created a simulated video recording and made a well-known artist "say" terrorism-supporting texts in it. In reality, this artist never made such a call. This video spread virally on social networks and was seen by many people. This action will result in criminal liability for the creator of the forged video directly, while the artist will not be punished. However, if both acted in prior agreement with unified intent, then the picture changes and both will be held accountable.

What legal consequences do other so-called third parties face if they like or share this video on social networks? It would be difficult to evaluate simply liking a post as perpetration. This, unlike the action of the post creator, is not an action of sufficient intensity and cannot create a clear, direct, and substantial threat, which is a necessary objective prerequisite of Article 330¹ of the Criminal Code. By liking such a shared video on social networks, the second person cannot become a perpetrator of the crime. By their actions, they do not generate any new threat. The situation changes when sharing a terrorism-supporting video on one's own page. This action makes the material additionally distributed and potentially accessible to people who might not have seen the video before sharing.⁴⁹

The same approaches can be applied to hate-motivated crimes as well. For example, such is racial discrimination punishable under Article 142¹ of the Criminal Code of Georgia, that is, an act committed with the aim of inciting national or racial hatred or discord, degrading national honor and dignity, as well as direct or indirect restriction of human rights based on race, skin color, national or ethnic affiliation, or granting advantages to humans on the same grounds, which substantially violated their rights. The legislator does not specify the methods of committing the crime.⁵⁰ Accordingly, it is entirely possible to commit racial discrimination through social networks using videos or other materials created with artificial intelligence.⁵¹

4. Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence and Georgian Criminal Law

This directive⁵² issued by the European Parliament and Council is also important for Georgian criminal legislation, as the Europeanization of Georgian criminal law and modification of its individual norms in accordance with EU directives has been ongoing for a long time. Georgia's cooperation with the European Union as an independent state began in 1996 with the signing of the Partnership and Cooperation Agreement, culminating in the Association Agreement in 2016.⁵³ We will not focus here on various treaties between Georgia and the European Union, however, overall, the implementation of criminal law directives issued within the EU framework has been continuously incorporated into Georgian domestic law. Accordingly, Georgia will also face the issue of implementing the directive on combating violence against women and domestic violence.

⁴⁹ Jishkariani, B., "Social Networks as a Challenge in Criminal Law", #4(80), „Justice and Law“, 2023, p. 75.

⁵⁰ Tsikarishvili, K. in Dvalidze, I., Kharanauli, L., Tumanishvili, G., Tsikarishvili, K., „Crimes against Human Rights and Freedoms according to the Criminal Code of Georgia“, "Meridiani", 2019, p. 42.

⁵¹ Jishkariani, B., "Social Networks as a Challenge in Criminal Law", #4(80), „Justice and Law“, 2023, p. 78.

⁵² ABL L 2024/1385, 24.05.2024, p. 1.

⁵³ Jishkariani, B., „European Criminal Law within the European Union“, "World of Lawyers", 2018, p. 20-21.

The aim of this article is not to provide a comprehensive analysis of this directive; therefore, we will briefly discuss specific actions that should be reflected in criminal legislation of EU member states and, due to the partnership, in Georgia as well. These are: female genital mutilation (Article 3 of the directive), forced marriage (Article 4), non-consensual sharing of intimate images or similar materials (Article 5), cyber-stalking (Article 6), cyber-harassment (Article 7), incitement to hatred and violence online (Article 8).

Based on the Council of Europe Convention on preventing and combating violence against women and domestic violence of May 11, 2011 (Istanbul Convention), the Criminal Code of Georgia already contains provisions on female genital mutilation (Article 133²) and forced marriage (Article 150¹).⁵⁴ However, regarding the distribution or manipulation of materials containing images of others, as we have already noted in previous parts of the article, there are significant deficits in Georgian criminal legislation. For example, Article 5(1)(b) of the directive requires the criminalization of the following acts: producing, manipulating or altering images, videos or similar material that creates the impression that a person is engaging in explicit sexual activities and subsequently distributing them publicly through information and communication technologies without that person's consent, if such actions are likely to cause serious harm to that person. Therefore, if tight legal cooperation with the EU continues, these actions should also be reflected as crimes in Georgian criminal legislation.

The directive goes even further and considers threats of such actions as criminal offenses when used to force the victim to perform or refrain from performing any action (Article 5 (1), c). Such a composition of duress, in the form of a special article, is unknown to Georgian legislation. However, extortion of property or forced marriage through this method is punishable. Moreover, relevant would be Article 151 of the Criminal Code of Georgia, the general composition of duress. Accordingly, there will be no significant deviation between Georgian and European provisions in this regard.

Furthermore, according to Article 7(a) of the directive, repeated or continuous threats made against a person using information and communication technologies should be punishable, at least when these actions are related to threats of crime and if these actions are likely to cause serious fear regarding the safety of oneself or dependent persons. According to the content of the directive, this threat might even occur through Deep Fake materials using artificial intelligence. Although Article 151 of the Georgian Criminal Code also addresses threats, its objective composition is quite narrowly formulated and includes only threats of death, bodily harm, or property destruction. Threats against other legal goods remain unpunished. The EU directive is formulated much more broadly, and Georgian legislation will need to be reconsidered in this regard.

Conclusion

Overall, to briefly assess the current situation, Georgian criminal legislation requires new comprehension in relation to modern technologies, whether through legislative changes or new interpretations of existing norms. However, we should note that this is not a deficiency unique to our legislation, as new technologies, especially artificial intelligence, pose new challenges to the entire world. At the bare minimum, based on obligations taken before the European Union, Georgia will face the need to implement relevant legislative changes. However, even without this obligation, it is clear that such important legal interests of people as personal autonomy, dignity, and freedom of action remain even more vulnerable in conditions where artificially manipulated materials can be more easily misused.

⁵⁴ Jishkariani, B., „Istanbul Convention and its Impacts on Georgian Criminal Law“, in the collection Jishkariani, B., Wassmer, M. (editors), „Criminal Law and Human Rights“, „University of Georgia Press“, 2019, p. 44.

Bibliography

1. Group of authors, Todua, Nona, Ivanidze, Maia, Turava, Merab (editors), General Part of Criminal Law, Commentary (Volume 2), Tbilisi, „Kalmosani“, 2021;
2. Dvalidze, Irakli, Kharanauli, Levan, Tumanishvili, Giorgi, Tsikarishvili, Kakha, Crimes against Human Rights and Freedoms according to the Criminal Code of Georgia, Tbilisi, Publishing House "Meridiani", 2019;
3. Cornelius, Kai, Criminal Law Challenges of Artificial Intelligence, in collection Jishkariani, Bachana, Wassmer, Martin (editors), Criminal Law and Human Rights, Tbilisi, "World of Lawyers", 2024;
4. Lekveishvili, Mzia, Mamulashvili, Gocha, Todua, Nona, Criminal Law Special Part (Book 1, Part Two), Tbilisi, "Meridiani", 2023;
5. Lekveishvili, Mzia, Mamulashvili, Gocha, Todua, Nona, Criminal Law Special Part (Book 2), Tbilisi, "Meridiani", 2020;
6. Mtchedlishvili-Hädrich, Ketevan, Criminal Law, General Part, Individual Forms of Crime Manifestation, Tbilisi, "Meridiani", 2011;
7. Decision of the Constitutional Court of Georgia №1/8/926, on the case of Giorgi Logua vs. Parliament of Georgia-
<https://matsne.gov.ge/ka/document/view/5609438?publication=0#DOCUMENT:1>; [last seen 18.02.2025];
8. Jorbenadze, Sergi, Defamation on Social Media and Means of Legal Protection in Georgian Court Practice, in Jishkariani, Bachana, Wassmer, Martin (editors), Criminal Law and Human Rights, Tbilisi, "World of Lawyers", 2023;
9. Jishkariani, Bachana, Istanbul Convention and its Impacts on Georgian Criminal Law, in the collection Jishkariani, Bachana, Wassmer, Martin (editors), Criminal Law and Human Rights, Tbilisi, „University of Georgia Press", 2019;
10. Jishkariani, Bachana, Social Networks as a Challenge in Criminal Law, Journal Justice and Law, #4(80), 2023.
11. Jishkariani, Bachana, Special Part of Criminal Law, Crimes against Property, Tbilisi, "World of Lawyers", 2024;
12. Jishkariani, Bachana, Special Part of Criminal Law, Crimes Against the person, Tbilisi, "World of Lawyers", 2022;
13. Jishkariani, Bachana, Stalking in Georgian Criminal Law, in the collection Jishkariani, Bachana, Wassmer, Martin (editors), Criminal Law and Human Rights, Tbilisi, "Lawyers' World", 2023;
14. Jishkariani, Bachana, European Criminal Law within the European Union, Tbilisi, "World of Lawyers", 2018;
15. Loladze, Besik, Phirtskhalashvili, Anna, Fundamental Rights, Tbilisi, "Forma", 2023;
16. Busche, Daniel, Einführung in die Rechtsfragen der künstlichen Intelligenz, Juristische Ausbildung, 2023;
17. Eisele Jörg, Duman, Irmak, Criminal Liability of Deepfake Pornography under Turkish and German Criminal Law, Zeitschrift für Internationale Strafrechtswissenschaft, #1, 2025;
18. Heinelt, Christian, Sind Fake-Bewertungen strafbar? Strafbarkeit fingierter Kundenbewertungen aus Sicht der Ersteller und der Betreiber von Bewertungsplattformen, Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT, 2022;
19. Lackner, Karl, Kühl, Kristian, Heger, Martin, StGB, München, „Beck“, 2023;
20. Lantwin, Tobias, Strafrechtliche Bekämpfung missbräuchlicher Deep Fakes, Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT, 2020;
21. Rößling, Fabian, Regulierung von Deep Fakes. Manipulierte Medien in AI Act, DS-GVO und allgemeinem Persönlichkeitsrecht, Zeitschrift für Digitalisierung und Recht, 2024;
22. Satzger, Helmut, Schluckebier, Wilhelm, Werner, Raik, (Ed.), StGB Kommentar, Köln, „Carl Heymans Verlag“, 2024;

23. Schönke, Adolf, Schröder, Horst, Strafgesetzbuch, München, „Beck“, 2019;
24. Steege, Hans, Haftung für Künstliche Intelligenz im Straßenverkehr, Straßenverkehrsrecht, 2023;
25. Thiel, Markus, „Deepfakes“ – Sehen heißt glauben? Zeitschrift für Rechtspolitik, 2021;
26. Tilson, Luke B., Eichinger, David, KI-generierte Deepfakes und ihre Gefahr für Kapitalmärkte, Zeitschrift für Bank und Kapitalmarktrecht, 2024;
27. v. Heintschel-Heinegg, Bernd, Kudlich, Hans, BeckOK StGB, 64. Edition, München, „Beck“, 2025;
28. Waxnegger, Kerstin, Künstliche Intelligenz und Strafrecht, Wien, „Österreich“, 2024;
29. Weber, Klaus (Ed.), Weber Kompakt, Rechtswörterbuch, München, „Beck“, 2024.