NORTHERN IRELAND HUMAN RIGHTS COMMISSION

Response to Department of Justice Consultation on Proposals to Criminalise Sexually Explicit Deepfake Images

October 2025

Table of Contents

Summary of Recommendations

The NIHRC recommends that the Department of Justice:

2.21 ensures that the proposed legislation is designed and implemented in a way that effectively protects victims from the online activities of third parties and safeguards their meaningful participation in public life, both online and offline. This requires a gender-sensitive approach.

2.22 ensures that the proposed legislation provides for effective remedies for victims of deepfakes, in accordance with Article 13 of the ECHR.

2.31 ensures that the proposed legislation is aligned with the standards set out in UN CEDAW and the Istanbul Convention to address the digital dimension of gender-based violence, particularly regarding effective prevention, support for victims and a holistic response to non-consensual sexually explicit deepfakes.

2.35 ensures that legislation criminalising creating or requesting the creation, or sharing or threatening to share, non-consensual sexually explicit deepfakes is embedded in human rights law, including the standards applicable to digital gender-based violence. Also, that this is clear and adaptable to artificial intelligence developments, with a view to providing for meaningful redress for victims and ensuring that perpetrators are effectively investigated, prosecuted and convicted.

3.6 adopts a victim-centred approach in the design, implementation and monitoring of the legislation. This includes consideration of ensuring that a holistic approach is adopted.

3.10 adopts a gender-sensitive approach in the design, implementation and monitoring of the legislation, with due consideration of intersectionality.

3.14 includes a definition of consent within the legislation that ensures consent is freely given and addresses circumstances where informed consent has not been given.

3.19 clarifies whether the intention to control or coerce falls within the intention to cause 'humiliation, alarm or distress', or if an additional specific motive should be added to the proposed legislation. Alternatively, whether creating or requesting the creation, or sharing or threatening to share a non-consensual sexually explicit deepfake with the intention to control or coerce would be covered by the legislation on controlling and coercive behaviour instead.

3.23 considers extending the offences within the proposed legislation to include scenarios where the perpetrator is targeting a person who is close to the individual depicted in the image.

3.25 specifies within the proposed legislation that offences with the motive of obtaining sexual gratification can include the perpetrator's gratification or that of other individuals.

3.27 clarifies that the offences within the proposed legislation do not require proof of harm to protect victims from re-victimisation and excessive restrictions on prosecutions.

3.35 introduces within the proposed legislation a summary-only base offence of intentionally creating or requesting the creation or sharing or threatening to share a sexually explicit deepfake image without consent, or a reasonable belief in consent, regardless of motive.

3.36 includes within the proposed legislation a reasonable excuse defence to avoid over-criminalisation when sharing

this type of image is necessary for reporting, preventing, detecting, investigating, or prosecuting a crime, or for the administration of justice. This defence must be clearly defined and balanced, to ensure accountability without unintentionally criminalising individuals who report crimes.

3.37 ensures the proposed legislation does not create an unintended gap in protection for victims in NI compared to other UK jurisdictions.

3.42 includes a definition of sexually explicit deepfakes within the proposed legislation that is clear enough to capture and keep pace with rapidly evolving artificial intelligence technology and its different uses, with a view to ensuring that victims are adequately protected.

3.47 includes within the proposed legislation express mention of the best interests of the child principle, as a primary consideration, regarding child offenders.

3.53 introduces specific provisions within the proposed legislation that assist law enforcement agencies and victims to remove non-consensual sexually explicit deepfakes from the internet to prevent re-victimisation.

3.54 ensures there is access to adequate compensation and appropriate redress mechanisms for harm caused by the creation or sharing of non-consensual sexually explicit deepfakes, particularly when removing content is unsuccessful or ineffective.

3.59 has a clear plan, with committed resources in place, to ensure up-to-date specialised training is available and provided as required (including refresher training) to relevant professionals and anyone who may come in contact with victims or deal with a complaint during a victim's journey through the criminal justice system. This training should be sensitive to gender-based violence and sexual abuse, as well as to the experiences of marginalised

groups such as disabled persons, lesbian, gay, bisexual, transgender, queer or questioning, intersex, asexual persons, children, and persons of national or ethnic minority backgrounds.

3.60 ensures that there is adequate capacity within law enforcement agencies to detect deepfakes and facilitate the collection of evidence, to enable effective investigations and prosecutions.

3.64 has a clear plan, with committed resources in place, for promoting education and awareness raising initiatives, focusing on prevention and encouraging reporting, the meaning of consent, healthy relationships, and the prevention of gender-based violence. It should also address privacy, promote non-discrimination and gender equality, digital literacy and online safety.

3.71 works with the NI Executive to ensure the integration of a human rights-based approach into the deployment of artificial intelligence systems by businesses into their operations, products and services. This includes ensuring that businesses are required to undertake robust content moderation and removal through proactively identify risks of harm, taking effective measures to address incidents, and cooperating with law enforcement agencies, civil society, and public authorities in NI and internationally to protect individuals from harm and prevent re-victimisation.

3.72 introduces a ban on online platforms that primarily facilitate the creation of non-consensual sexually explicit deepfake content, such as tools marketed as 'nudifying' services to protect people at risk of becoming victims or offenders.

1.0 Introduction

1.1 The Northern Ireland Human Rights Commission (NIHRC), pursuant to section 69(1) of the Northern Ireland Act 1998, reviews the adequacy and effectiveness of law and practice relating to the protection of human rights in Northern Ireland (NI). In accordance with this function, the following advice is submitted in response to the Department of Justice's consultation on proposals to criminalise sexually explicit deepfake images.

1.2 The NIHRC bases its advice on the international human rights standards and treaty obligations of the United Nations (UN) and Council of Europe (CoE), including:

- CoE European Convention on Human Rights 1950 (ECHR);[1]
- UN Convention on the Elimination of All Forms of Racial Discrimination 1965 (UN CERD);[2]
- UN International Covenant on Civil and Political Rights 1966 (UN ICCPR);[3]
- UN Convention on the Elimination of all Forms of Discrimination against Women 1981 (UN CEDAW);[4]
- UN Convention against Torture 1984 (UN CAT);[5]
- UN Convention on the Rights of the Child 1989 (UN CRC);[6]
- CoE European Convention on Cybercrime 2001 (Budapest Convention);[7]
- UN Convention on the Rights of Persons with Disabilities 2006 (UN CRPD);[8]
- CoE Convention on Preventing and Combating Violence against Women and Domestic Violence 2011 (Istanbul Convention);[9] and

[1] Ratified by the UK in 1951.
[2] Ratified by the UK in 1969.
[3] Ratified by the UK in 1966.
[4] Ratified by the UK in 1986.
[5] Ratified by the UK in 1988.
[6] Ratified by the UK in 1989.
[7] Ratified by the UK in 2011.
[8] Ratified by the UK in 2009.
[9] Ratified by the UK in 2022.

- CoE Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law.[10]

1.3 In addition to these treaty standards, the following declarations and principles provide further guidance in respect of specific areas:

- UN Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power;[11]
- UN Declaration on the Elimination of Violence against Women;[12]
- UN CEDAW Committee General Recommendation No 23: Political and Public Life;[13]
- UN Special Rapporteur on Violence Against Women, Its Causes and Consequences, Ms Radhika Coomaraswamy, 1997 Report;[14]
- UN Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law;[15]
- UN Human Rights Committee General Comment No 32;[16]
- UN Guiding Principles on Business and Human Rights;[17]
- UN CAT Committee General Comment No 3;[18]
- UN CRC Committee General Comment No 14;[19]
- CAT/C/GC/3, 'UN CAT Committee General Comment No 3: Implementation of Article 14 by States Parties', 13 December 2012, at para 21;
- UN Human Rights Committee General Comment No 35;[20]

[10] The UK signed the Council of Europe Framework Convention on Artificial Intelligence on 5 September 2024 but has yet to ratify it.
[11] UN Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power, 29 November 1985.
[12] UN General Assembly, 'Declaration on the Elimination of Violence Against Women', 20 December 1993.
[13] A/52/38, 'UN CEDAW Committee General Recommendation No 23: Political and Public Life', 1997.
[14] E/CN.4/1997/47, 'Report of the UN Special Rapporteur on Violence Against Women, Its Causes and Consequences, Ms Radhika Coomaraswamy', 12 February 1997, at para 22.
[15] UN General Assembly, 'UN Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law', 16 December 2005.
[16] CCPR/C/GC/32, 'UN Human Rights Committee General Comment No 32: Right to Equality Before the Courts and Tribunals and to a Fair Trial', 23 August 2007.
[17] Office of the High Commissioner for Human Rights, 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework' (OHCHR, 2011).
[18] CAT/C/GC/3, 'UN CAT Committee General Comment No 3: Implementation of Article 14 by States Parties', 13 December 2012.
[19] CRC/C/GC/14, 'UN CRC Committee General Comment No 14: Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration', 29 May 2013.
[20] CCPR/C/GC/35, 'UN Human Rights Committee General Comment No 35: Liberty and Security of Person', 16 December 2014.

- UN CEDAW Committee General Recommendation No 35;[21]
- UN CEDAW Committee Concluding Observations 2019;[22]
- UN CAT Committee 2019 Concluding Observations on the UK;[23]
- CoE GREVIO Committee General Recommendation No 1;[24]
- UN General Assembly Resolution on preventing and eliminating violence against women and girls in the digital environment;[25] and
- UN Working Group on Business and Human Rights Report on artificial intelligence procurement and deployment.[26]

1.4 The NIHRC welcomes the opportunity to consider and provide advice on the Department of Justice's proposal to criminalise the creation and sharing of non-consensual sexually explicit deepfake images of adults.

2.0 Criminalising Non-consensual Sexually Explicit Deepfakes

2.1 The Department of Justice is proposing to make it an offence to intentionally create, or request the creation of, a sexually explicit deepfake image of an adult, without consent, with the intention of causing humiliation, alarm or distress to the person depicted in the image, or for the purposes of sexual gratification.[27] The Department of Justice is also proposing to make it an offence to intentionally share a sexually explicit deepfake image of an adult, without

[21] CEDAW/C/GC/35, 'UN CEDAW Committee General Recommendation No 35: Gender-based Violence Against Women, Updating General Recommendation No 19', 26 July 2017.
[22] CEDAW/C/GBR/CO/8, 'UN CEDAW Committee Concluding Observations on the UK Eighth Periodic Report', 8 March 2019.
[23] CAT/C/GBR/CO/6, 'UN CAT Committee Concluding Observations on the Sixth Periodic Report of the UK of Great Britain and NI', 7 June 2019.
[24] GREVIO(2021)20, 'CoE GREVIO Committee General Recommendation No 1: Digital Dimension of Violence Against Women' (GREVIO, 2021).
[25] A/RES/79/152, 'UN General Assembly Resolution on Intensification of Efforts to Prevent and Eliminate All Forms of Violence Against Women and Girls: The Digital Environment', 17 December 2024.
[26] A/HRC/59/53, 'UN Working Group on Business and Human Rights Artificial Intelligence Procurement and Deployment: Ensuring Alignment with the Guiding Principles on Business and Human Rights - Report of the Working Group on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises' (OHCHR, 2025).
[27] Department of Justice, 'A Consultation on Proposals to Criminalise Sexually Explicit Deepfake Images' (DoJ, 2025).

consent, with the intention of causing humiliation, alarm or distress to the person depicted in the image, or for the purposes of sexual gratification, or threaten to share these images with the intent to cause fear or distress to the person depicted in the image.[28]

2.2 In general, the NIHRC welcomes the criminalisation of non-consensual sexually explicit deepfakes from a human rights perspective. This is from several aspects regarding human rights obligations, which are set out below. However, there are some further considerations which are also set out in detail below, where relevant.

European Convention on Human Rights

2.3 As identified by the Department of Justice, criminalising online activity to create non-consensual sexually explicit deepfakes engages Articles 8 (right to respect for private and family life)[29] and 10 (freedom of expression)[30] of the ECHR. The new criminal offences also engage Articles 5 (right to liberty and security)[31] and 7 (no punishment without law) of the ECHR.[32]

2.4 Article 8 of the ECHR protects individuals from arbitrary interferences by public authorities in their private and family life, home, and correspondence.[33] States may limit this right under Article 8(2) of the ECHR, if the actions are in accordance with the law and necessary in a democratic society for specific objectives outlined in this provision.[34] The prevention of crime and the protection of the rights and freedoms of others are some of those objectives contained within Article 8(2) of the ECHR. The European Court of Human Rights (ECtHR) has clarified that restrictive

[28] Ibid.
[29] See also Article 17, UN ICCPR; Article 22, UN CRPD; Article 16, UN CRC.
[30] See also Article 19, UN ICCPR; Article 21, UN CRPD; Article 13, UN CRC.
[31] See also Article 9, UN ICCPR; Article 14, UN CRPD; Article 37(b), UN CRC.
[32] See also Article 15, UN ICCPR; Article 40(2)(a), UN CRC.
[33] *Libert v France* (2018) ECHR 185.
[34] Article 8(2) of the ECHR states that "there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

measures must have a reasonable relationship of proportionality between the means employed and the aim sought.[35]

2.5 In its consultation, the Department of Justice assessed how criminalising some online activity that could also trigger sex offender notification requirements may restrict Article 8 of the ECHR.[36] The Department of Justice believes these interferences are justified in pursuit of the legitimate aims of preventing crime and protecting the rights of others.[37] As such, the Department of Justice considers these measures to be proportionate.[38]

2.6 Similarly, and as highlighted by the Department of Justice, the new offences could engage Article 10 of the ECHR by limiting defendants' freedom to hold opinions and share information without interference from public authorities.[39] Article 10 of the ECHR "protects not only the substance of the ideas and information expressed, but also the form in which they are conveyed".[40] Furthermore, the Internet provides an "unprecedented platform for the exercise of freedom of expression… enhancing the public's access to news and facilitating the dissemination of information generally".[41]

2.7 As a qualified right, Article 10 of the ECHR may be subject to restrictions prescribed by law, where that is necessary in a democratic society to achieve one of the legitimate aims set out in Article 10(2) of the ECHR.[42] These legitimate aims include preventing crime and protecting the rights and reputation of others.[43] This is particularly relevant when it comes to the publication of images, especially when they contain "very personal or even intimate information about an individual or his or her [or

[35] *Dudgeon v UK* (1983) ECHR 2, at paras 51-53; *Phillips v UK* (2001) ECHR 437, at paras 51-52.
[36] Department of Justice, 'A Consultation on Proposals to Criminalise Sexually Explicit Deepfake Images' (DoJ, 2025), at 26.
[37] Ibid.
[38] Ibid.
[39] Ibid.
[40] *Karatas v Turkey* (1999) ECHR 47, at 49.
[41] *Delfi AS v Estonia* (2015) ECHR 586, at paras 110 and 133.
[42] Article 10(2) of the ECHR states that "the exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary".
[43] Article 10(2), ECHR.

their] family".[44] Also, where the images "are taken on private premises and clandestinely through the use of secret recording devices".[45] The ECtHR has further clarified that:

> a person's image constitutes one of the chief attributes of his or her [or their] personality, as it reveals the person's unique characteristics and distinguishes the person from his or her [or their] peers. The right to protection of one's image is thus one of the essential components of personal development. It mainly presupposes the individual's right to control the use of that image, including the right to refuse publication.[46]

2.8 Furthermore, non-consensual sexually explicit deepfakes can restrict a victim's freedom of expression under Article 10 of the ECHR. This includes:

> freedom of artistic expression – notably within freedom to receive and impart information and ideas – which affords the opportunity to take part in the public exchange of cultural, perform, distribute or exhibit works of art contribute to the exchange of ideas and opinions which is essential for a democratic society… It must be remembered that Article 10 [of the ECHR] protects not only the substance of the ideas and information expressed but also the form in which they are conveyed.[47]

2.9 Article 10 of the ECHR may require States to "create… a favourable environment for participation in public debate of all persons concerned, enabling them to express their opinions and ideas without fear".[48] Research shows that women are often the main target of non-consensual sexually explicit deepfakes[49] and that such deepfakes can be weaponised with a view to intimidating,

---

[44] *Von Hannover v Germany (No 2)* (2012) ECHR 228, at para 103; *Mosley v UK* (2011) ECHR 774, at para 115.
[45] Ibid.
[46] *Von Hannover v Germany (No 2)* (2012) ECHR 228, at para 96.
[47] *Karatas v Turkey* (1999) ECHR 47, at 49; *Handyside v UK* (1990) ECHR 32.
[48] *Khadija Ismayilova v Azerbaijan* (2019) ECHR 11, at para 158.
[49] Security Hero, '2023 State of Deepfakes: Realities, Threats, and Impact'. Available at: https://www.securityhero.io/state-of-deepfakes/

discrediting and silencing the victim.[50] For example, non-consensual sexually explicit deepfakes can have a "silencing effect" with victims self-censoring and feeling discouraged from engaging in public debate and online activity, due to a fear that these images will be created and shared.[51] In NI, there are several documented cases of women journalists and politicians who have experienced the publication of deepfakes with their image in the context of reporting on issues of public interest, or during political campaigns.[52] In the case of *Khadija Ismayilova v Azerbaijan* (2019), the ECtHR found a violation of Articles 8 and 10 of the ECHR for the State's failure to protect the applicant when intimate videos of her recorded covertly were disseminated online in an attempt to intimidate her.[53]

2.10 The Department of Justice considers the proposed restrictions on freedom of expression compatible with Article 10 of the ECHR and justified as necessary and proportionate measures to protect individuals from the harms caused by non-consensual sexually explicit deepfake images.[54]

2.11 Based on the information provided in the consultation document, the NIHRC has no concerns with the Department of Justice's assessment of the proposed offences' restrictions on Articles 8 and 10 of the ECHR. However, the Department of Justice needs to satisfy itself that the proposals strike a fair balance between the interests and rights at stake, both at the time of introducing the offences into a Justice Bill and in the event of any amendments made during its passage through the NI Assembly.

2.12 Criminal offences that could attract prison penalties also engage Articles 5 and 7 of the ECHR. Article 5 of the ECHR includes the

[50] Can Yavuz, 'Adverse Human Rights Impacts of Dissemination of Nonconsensual Sexual Deepfakes in the Framework of the ECHR: A Victim-Centered Perspective' (2025) 56 *Computer Law and Security Review*, at 13.
[51] Ibid.
[52] Equality Now, 'Tech-facilitated Gender-based Violence'. Available at: *Tech-facilitated gender-based violence (TFGBV) | Equality Now*; Cara Hunter, 'How a Deepfake Almost Ruined My Political Career', TED Talk, 19 October 2024; Jim Waterson, 'British female politicians targeted by fake pornography', *The Guardian*, 1 July 2024; Can Yavuz, 'Adverse Human Rights Impacts of Dissemination of Nonconsensual Sexual Deepfakes in the Framework of the ECHR: A Victim-Centered Perspective' (2025) 56 *Computer Law and Security Review*, at 13-14.
[53] *Khadija Ismayilova v Azerbaijan* (2019) ECHR 11.
[54] Department of Justice, 'A Consultation on Proposals to Criminalise Sexually Explicit Deepfake Images' (DoJ, 2025), at 28.

principle of legal certainty, clarifying that it is not only about the existence of a law, but the "quality of the law".[55] Thus:

> the 'quality of law' implies that where a national law authorises a deprivation of liberty, it must be sufficiently accessible, precise and foreseeable in its application to avoid all risk of arbitrariness. The standard of 'lawfulness' set by the [ECHR]… requires that all law be sufficiently precise to allow the person – if need be, with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.[56]

2.13 The UN Human Rights Committee has also stated that "any substantive grounds for arrest or detention must be prescribed by law and should be defined with sufficient precision to avoid overly broad or arbitrary interpretation or application".[57]

2.14 While the above focuses on a deprivation of liberty scenario, the obligations outlined are beneficial in the broader context of understanding the principle of legal certainty.

2.15 Criminal offences must also comply with Article 7 of the ECHR, which requires offences and penalties to be clearly defined by law. Offences' definitions and penalties must also be "reasonably… foreseen".[58] The ECtHR has stated that, under Article 7 of the ECHR, 'quality of law' is a key consideration regarding offence definitions and penalties.[59] This requires law to have "sufficient precision as to enable the [individual]… to discern, even with appropriate advice, to a degree that was reasonable in the circumstances".[60]

---

[55] The UN Human Rights Committee has also emphasised that grounds for arrest or detention must be defined by law and specified clearly to prevent broad or arbitrary interpretation. See *Del Río Prada v Spain* (2013) ECHR 1004, at para 125; *Medvedyev and Others v France* (2010) ECHR 384, at para 80; CCPR/C/GC/35, 'Human Rights Committee General Comment No 35: Article 9', 16 December 2014, at para 22.
[56] *Del Río Prada v Spain* (2013) ECHR 1004, at para 125; *Medvedyev and Others v France* (2010) ECHR 384, at para 80.
[57] CCPR/C/GC/35, 'Human Rights Committee General Comment No 35: Article 9', 16 December 2014, at para 22.
[58] *Jorgic v Germany* (2007) ECHR 583, at paras 103-114; *Kafkaris v Cyprus* (2008) ECHR 143, at para 150.
[59] *Kafkaris v Cyprus* (2008) ECHR 143, at paras 150-152.
[60] Ibid.

2.16 This would be the first time this type of image-based sexual abuse is criminalised in NI. In line with the obligations of Articles 5 and 7 of the ECHR, the Department of Justice needs to ensure the law is clear and accessible, with a view to individuals being able to anticipate the consequences of their online activity, and that the offences do not unintentionally catch situations that should not be criminalised (such as actions needed to report a crime). The NIHRC has no general concerns with the clarity of the proposed offences, notwithstanding some specific issues raised below, particularly regarding motives and the definition of sexually explicit deepfake images.

2.17 Additionally, failure to tackle image-based sexual abuse effectively could engage a victim's rights under Articles 3 (freedom from torture and ill treatment),[61] 13 (right to an effective remedy)[62] and 14 (prohibition of discrimination)[63] of the ECHR. In extreme cases that lead to a threat to life or actual loss of life, it could also engage Article 2 (right to life) of the ECHR.[64]

2.18 Depending on the severity, rights under Articles 2, 8, and/or 3 of the ECHR can be restricted in the context of sexual abuse. The ECtHR has held that States have a responsibility to protect individuals from violence by third parties.[65] This has been particularly true in cases involving victims of domestic violence.[66] Under Article 8 of the ECHR, States have a duty to protect the physical and moral integrity of individuals from other persons,[67] which requires establishing an adequate legal framework affording protection against acts of violence by private individuals.[68] Article 8 of the ECHR also protects an individual's image as an essential component of personal development.[69] The ECtHR has found that information regarding intimate or sexual life is highly private information protected by a high threshold regarding publication

[61] See also Article 7, UN ICCPR; Article 2, UN CAT; Article 15, UN CRPD; Article 37(a), UN CRC.
[62] See also Article 2, UN ICCPR; Article 6, UN CERD; Article 14, UN CAT; Article 13, UN CRPD.
[63] See also Article 26, UN ICCPR; Article 2(2), UN ICESCR; Article 2, UN CRC; UN CERD; UN CEDAW; UN CRPD.
[64] See also Article 6, UN ICCPR; Article 10, UN CRPD; Article 6, UN CRC.
[65] *C v Romania* (2022) ECHR 635, at paras 62-66.
[66] *Buturugă v Romania* (2020) ECHR 136.
[67] Including cyberbullying by a person's intimate partner. See *Buturugă v Romania* (2020) ECHR 136, at paras 74, 78-79; *Volodina v Russia* (No 2) (2021) ECHR 745, at paras 48-49; *MȘD v Romania* (2024) ECHR 887, at paras 118-119; *Špadijer v Montenegro* (2021) ECHR 921, at para 100; *C v Romania* (2022) ECHR 635, at paras 67-87.
[68] *Sandra Janković v Croatia* (2008) ECHR 24, at para 45.
[69] *López Ribalda and Others v Spain* (2019) ECHR 752, at paras 87-91.

without consent.[70] The ECtHR has determined that effective deterrence against serious acts, where fundamental values and essential aspects of private life are at stake, requires efficient criminal law provisions.[71]

2.19 It is also worth noting that the UN CAT Committee has specifically recommended that the UK Government and NI Executive "ensure all cases of gender-based violence are thoroughly investigated, alleged perpetrators prosecuted and, if convicted, punished appropriately. Also, that victims or their families receive redress, including adequate compensation".[72]

2.20 The legal framework in NI needs to deter image-based sexual abuse and protect victims effectively. Otherwise, victims' rights under Article 13 of the ECHR could also be engaged by the lack of an effective remedy against non-consensual sexually explicit deepfakes.[73] This places an obligation on national authorities to "protect human rights first and foremost within their own legal system".[74] This includes "preventing and putting right… violations" of the ECHR.[75] Since women and girls are disproportionately harmed by these images, an ineffective legal framework could also restrict rights under Article 14 of the ECHR, in conjunction with Article 13 of the ECHR.[76]

2.21 The NIHRC recommends that the Department of Justice ensures that the proposed legislation is designed and implemented in a way that effectively protects victims from the online activities of third parties and safeguards their meaningful participation in public life, both online and offline. This requires a gender-sensitive approach.

---

[70] *Biriuk v Lithuania* (2008) ECHR 1528, at paras 39-42.
[71] *MC v Bulgaria* (2003) ECHR 646, at para 166; *Söderman v Sweden* (2013) ECHR 128.
[72] CAT/C/GBR/CO/6, 'UN CAT Committee Concluding Observations on the Sixth Periodic Report of the UK of Great Britain and NI', 7 June 2019, at para 57(a).
[73] *Kudła v Poland* (2000) ECHR 512, at para 152.
[74] Ibid.
[75] Ibid.
[76] Article 14 of the ECHR states that "the enjoyment of the rights and freedoms set forth in [the ECHR]… shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status". This means that Article 14 of the ECHR does not prohibit discrimination as such, but only discrimination in the enjoyment of the "rights and freedoms set forth in the Convention". Thus, Article 14 of the ECHR is not a 'free-standing' right, but is of an ancillary nature to other EHRC rights. See ECtHR, 'Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No 12 to the Convention' (CoE, 2025), at 7.

2.22 The NIHRC recommends that the Department of Justice ensures that the proposed legislation provides for effective remedies for victims of deepfakes, in accordance with Article 13 of the ECHR.

UN CEDAW and CoE Istanbul Convention

2.23 The NIHRC welcomes the Department of Justice's acknowledgement that the non-consensual creation and sharing of sexually explicit deepfakes is a gender-based problem affecting mostly women and girls.[77]

2.24 The UN CEDAW and Istanbul Convention stress the need to ensure that victim-centred and trauma-informed approaches are adopted in scenarios involving victims and survivors of abuse and/or violence.[78] This also requires ensuring that a gender-sensitive approach is adopted, where necessary.[79]

2.25 The UN CEDAW Committee recognises online and technology-facilitated violence as a form of gender-based violence against women that is within the scope of the UN CEDAW.[80] The UN CEDAW Committee has stated that:

> gender-based violence against women occurs in all spaces and spheres of human interaction, whether public or private, including… the redefinition of public and private through technology-mediated environments, such as contemporary forms of violence occurring online and in other digital environments. In all those settings, gender-based violence against women can result from acts or omissions of State or non-State actors.[81]

[77] Department of Justice, 'A Consultation on Proposals to Criminalise Sexually Explicit Deepfake Images' (DoJ, 2025).
[78] CEDAW/C/GC/35, 'UN CEDAW Committee General Recommendation No 35: Gender-based Violence Against Women, Updating General Recommendation No 19', 26 July 2017, at para 29(c)(i); CoE Convention on Preventing and Combating Violence Against Women and Domestic Violence 2011.
[79] Ibid.
[80] CEDAW/C/GC/35, 'UN CEDAW Committee General Recommendation No 35: Gender-based Violence Against Women, Updating General Recommendation No 19', 26 July 2017, at para 20.
[81] Ibid.

2.26 The UN CEDAW Committee has also confirmed that gender-based violence against women is a form of discrimination.[82] States have an obligation to eliminate all acts of discrimination against women perpetrated by State actors or third parties, including individuals, organisations, or companies.[83] Regarding the 'silencing effect' of deepfakes mentioned above, the UN CEDAW specifically protects women's right to participation in public and political life.[84]

2.27 The Istanbul Convention provides a European framework for protection against all forms of gender-based violence against women. It can also be used as an indicator of best practice and provide guidance on how to develop legislation in relation to sexual offences more broadly.[85]

2.28 The CoE Group of Experts on Action against Violence Against Women and Domestic Violence (CoE GREVIO Committee) clarifies that:

> non-consensual image or video sharing, coercion and threats, including rape threats, sexualised bullying and other forms of intimidation, online sexual harassment, impersonation, online stalking or stalking via the Internet of Things as well as psychological abuse and economic harm perpetrated via digital means against women and girls all come under the… definition [of violence against women].[86]

2.29 The CoE GREVIO Committee recommends that States address this issue holistically, with a focus on prevention, protection, prosecution, and coordinated policies.[87]

2.30 Therefore, the Istanbul Convention sets the minimum standard for a holistic response to address online and offline violence against women that includes taking steps to prevent through awareness

[82] Ibid, at para 21.
[83] Ibid.
[84] Article 7, UN Convention on the Elimination of All Forms of Discrimination against Women 1981; A/52/38, 'UN CEDAW Committee General Recommendation No 23: Political and Public Life', 1997.
[85] See Articles 33, 34, 35, 36, 40 and 49 of the Istanbul Convention.
[86] GREVIO(2021)20, 'CoE GREVIO Committee General Recommendation No 1: Digital Dimension of Violence Against Women' (GREVIO, 2021), at para 33.
[87] Article 7, Istanbul Convention; GREVIO(2021)20, 'CoE GREVIO Committee General Recommendation No 1: Digital Dimension of Violence Against Women' (GREVIO, 2021).

raising and education, training professionals and intervention programmes for perpetrators, and tackling attitudes that perpetuate violence against women and girls. Also, a victim-centred approach must be adopted to protect and support victims and individuals at risk. Furthermore, investigations and criminal proceedings must be pursued to bring perpetrators to justice and ensure accountability.[88]

2.31 The NIHRC recommends that the Department of Justice ensures that the proposed legislation is aligned with the standards set out in UN CEDAW and the Istanbul Convention to address the digital dimension of gender-based violence, particularly regarding effective prevention, support for victims and a holistic response to non-consensual sexually explicit deepfakes.

CoE Budapest Convention and the CoE Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law

2.32 The Budapest Convention focuses on cybercrime and electronic evidence. It requires States to criminalise internet and computer-based offences and improve investigative techniques to secure electronic evidence, and to facilitate international co-operation regarding investigation or proceedings.[89]

2.33 As a relatively new treaty, the CoE Framework Convention on Artificial Intelligence, has been signed, but not yet ratified by the UK. By taking this step the UK has agreed to "not defeat the object and purpose of the treaty".[90] The CoE Framework Convention aims

[88] Article 5(2) of the Istanbul Convention requires States to take the necessary legislative and other measures to exercise due diligence in preventing, investigating, punishing, and providing reparation for acts of violence covered by the Convention perpetrated by non-state actors. Similarly, Article 49 of the Istanbul Convention requires States to ensure that investigations and judicial proceedings are carried out without undue delay while taking into consideration the rights of the victim during all stages of the criminal proceedings and having regard to the gendered understanding of violence.
[89] CoE European Convention on Cybercrime (Budapest Convention); Adriane van der Wilk, 'Protecting Women and Girls from Violence in the Digital Age: The Relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women' (CoE, 2021), at 17.
[90] Article 18, Vienna Convention on the Law of Treaties 1969.

to ensure that all activities involved in artificial intelligence systems respect human rights, democracy, and the rule of law, while supporting technological progress and innovation. The CoE Framework Convention requires States to ensure "that activities within the lifecycle of artificial intelligence systems are fully consistence with human rights, democracy and the rule of law".[91] It also requires State Parties to:

> assess the need for a moratorium or ban or other appropriate measures in respect of certain uses of artificial intelligence systems where it considers such uses incompatible with the respect for human rights, the functioning of democracy or the rule of law.[92]

2.34 The NIHRC welcomes the Department of Justice's efforts to address the harmful human rights effects of artificial intelligence-facilitated sexual abuse in the proposed consultation document. However, the Department of Justice needs to ensure that the investigative techniques aimed at tackling the proposed offences are effective to secure proceedings and, eventually, convictions. The legislation needs to clearly address and protect against the different risks posed by artificial intelligence deployment and be flexible to adapt to new developments in the technology.

2.35 The NIHRC recommends that the Department of Justice ensures that legislation criminalising creating or requesting the creation, or sharing or threatening to share, non-consensual sexually explicit deepfakes is embedded in human rights law, including the standards applicable to digital gender-based violence. Also, that this is clear and adaptable to artificial intelligence developments, with a view to providing for meaningful redress for victims and ensuring that perpetrators are effectively investigated, prosecuted and convicted.

[91] Article 1(1), CoE Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law 2024.
[92] Article 16(4), CoE Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law 2024.

3.0 Specific Issues within the Proposals to Criminalise Sexually Explicit Deepfake Images

Victim-centred approach

3.1 Victims of image-based sexual abuse can suffer severe psychological harm, harassment, damage to their reputation and career, and even financial losses due to extortion or legal actions taken to seek remedies.[93]

3.2 Despite acknowledging the particularly harmful consequences of non-consensual sexually explicit deepfakes for victims, the Department of Justice's proposals do not explicitly include a victim-centred approach to the legislation.

3.3 A victim-centred approach is advocated within the UN CEDAW.[94] Similarly, the Istanbul Convention provides that States must take measures to protect the rights and needs of victims throughout judicial proceedings, including "providing for their protection, as well as that of their families and witnesses, from intimidation, retaliation and repeat victimisation".[95]

3.4 According to the UN Basic Principles of Justice for Victims of Crime and Abuse of Power "victims should be treated with compassion and respect for dignity".[96] The UN Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims also provides that

[93] Felipe Romero Moreno, 'Generative Artificial Intelligence and Deepfakes: A Human Rights Approach to Tackling Harmful Content' (2024) 38 *International Review of Law, Computers and Technology* 297; Equality Now, 'Briefing Paper: Deepfake Image-based Sexual Abuse, Tech-facilitated Sexual Exploitation and the Law' (AUDRi, 2024), at 4; Mariëtte van Huijstee et al, 'Tackling Deepfakes in European Policy' (EPRS, 2021), at 30.
[94] CEDAW/C/GC/35, 'UN CEDAW Committee General Recommendation No 35: Gender-based Violence Against Women, Updating General Recommendation No 19', 26 July 2017, at para 32.
[95] Article 56, Istanbul Convention; GREVIO(2021)20, 'CoE GREVIO Committee General Recommendation No 1: Digital Dimension of Violence Against Women' (GREVIO, 2021).
[96] UN Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power, 29 November 1985, at Principle 4.

appropriate measures must be taken to ensure the safety, well-being and privacy of victims and their families and "that a victim who has suffered violence or trauma should benefit from special consideration and care to avoid his or her re-traumatisation".[97] The UN CAT Committee makes a similar recommendation and calls for sensitivity towards marginalised or high-risk groups or individuals for the purposes of preventing re-traumatisation and stigmatisation.[98]

3.5 Failure to provide appropriate protection for victims poses an obstacle to the right to an effective remedy.[99] Moreover, re-victimisation during criminal investigations and proceedings may inhibit victims from making complaints due to fears of secondary victimisation by the process.[100]

3.6 **The NIHRC recommends that the Department of Justice adopts a victim-centred approach in the design, implementation and monitoring of the legislation. This includes consideration of ensuring that a holistic approach is adopted.**

Gender-sensitive approach

3.7 The Department of Justice's consultation mentions that the non-consensual creation or request to create and sharing or threat to share sexually explicit deepfakes is a gender-based phenomenon affecting mostly women and girls.[101] The NIHRC welcomes this approach. However, consideration of intersectionality is missing.

---

[97] UN General Assembly, 'UN Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law', 16 December 2005, at Principle 10.
[98] CAT/C/GC/3, 'UN CAT Committee General Comment No 3: Implementation of Article 14 by States Parties', 13 December 2012, at paras 21, 33, 34 and 36.
[99] *Kudła v Poland* (2000) ECHR 512, at para 152; CAT/C/GC/3, 'UN CAT Committee General Comment No 3: Implementation of Article 14 by States Parties', 13 December 2012, at para 38; UN General Assembly, 'UN Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law', 16 December 2005, at Principle 3.
[100] *L and Others v France* (2025) ECHR 98, at paras 200 and 232; E/CN.4/1997/47, 'Report of the UN Special Rapporteur on Violence Against Women, Its Causes and Consequences, Ms Radhika Coomaraswamy', 12 February 1997, at para 22.
[101] Department of Justice, 'A Consultation on Proposals to Criminalise Sexually Explicit Deepfake Images' (DoJ, 2025).

3.8 Technology-facilitated gender-based violence is recognised as a form of gender-based discrimination. It is defined as:

> any act that is committed, assisted, aggravated, or amplified by the use of information communication technologies or other digital tools, that results in or is likely to result in physical, sexual, psychological, social, political, or economic harm, or other infringements of rights and freedoms.[102]

3.9 It is recognised that technology-facilitated gender-based violence can intersect with other grounds of discrimination.[103] Human rights law requires that an individual's specific characteristics or needs are considered and that, where necessary, positive action or special measures are taken to ensure that individuals are not discriminated against.[104] Article 6 of the Istanbul Convention highlights the need for gender-sensitive policies by stating that State Parties "shall undertake to include a gender perspective in the implementation and evaluation of the impact of the provisions of [the Istanbul] Convention and to promote and effectively implement policies of equality between women and men and the empowerment of women". The UN CEDAW Committee has also confirmed that this includes considering the intersectional dimension of discrimination when it comes to lesbian, gay, bisexual, transgender, queer or questioning, intersex and asexual persons, d/Deaf and disabled persons, racial and ethnic minorities, and children, among others.[105]

3.10 **The NIHRC recommends that the Department of Justice adopts a gender-sensitive approach in the design, implementation and monitoring of the legislation, with due consideration of intersectionality.**

[102] UN Women, 'Repository of UN Women's Work on Technology-Facilitated Violence Against Women and Girls (March 2025)' (UN Women, 2025), at 1.
[103] UN Women, 'Technology-facilitated Gender-based Violence: Developing a Shared Research Agenda' (UN Women, 2024), at 4.
[104] *Opuz v Turkey* (2009) ECHR 870.
[105] CEDAW/C/GC/28, 'UN CEDAW Committee General Recommendation No 28: Core Obligations of States Parties Under Article 2 of the UN CEDAW', at para 18; UN Women and others, 'Technology-facilitated gender-based violence: Developing a shared research agenda' (UN Women, 2024), at 4.

Consent

3.11 The NIHRC welcomes that the scope of the new offences will focus on non-consensual actions or lack of reasonable belief in consent as a requirement to attract criminal responsibility. However, the Department of Justice's consultation does not define consent or set out how to deal with consent not freely given.

3.12 The Istanbul Convention says consent "must be given voluntarily as the result of the person's free will assessed in the context of the surrounding circumstances".[106] UK data protection law also requires that consent must be freely given, specific, informed and unambiguous.[107]

3.13 A clear definition of consent in the legislation would be useful in addressing situations where consent might not be given freely, for example, in situations of fraud, duress, undue influence or mistake, including coercive control and domestic abuse.

3.14 **The NIHRC recommends that the Department of Justice includes a definition of consent within the legislation that ensures consent is freely given and addresses circumstances where informed consent has not been given.**

Potential gaps in the offences as described

3.15 Considering Articles 5 and 7 of the ECHR,[108] the NIHRC welcomes the intention to include descriptions of the offences in the legislation, as a way to provide clarity in the law. However, it would be beneficial for the Department of Justice to clarify some aspects of the offences, to ensure all relevant cases of gender-based

[106] Article 36(2), Istanbul Convention.
[107] Articles 4(11) and 7, UK General Data Protection Regulations 2018; Information Commissioner's Office, 'What is Valid Consent?'. Available at: What is valid consent? | ICO
[108] *Del Río Prada v Spain* (2013) ECHR 1004, at para 125; *Medvedyev and Others v France* (2010) ECHR 384, at para 80; CCPR/C/GC/35, 'UN Human Rights Committee General Comment No 35: Liberty and Security of Person', 16 December 2014, at para 22; *Jorgic v Germany* (2007) ECHR 583, at paras 103-114; *Kafkaris v Cyprus* (2008) ECHR 143, at para 150.

violence are covered, in line with UN CEDAW and Istanbul Convention.[109]

3.16 For example, the proposed offences do not include control or coercion as one of the motives for creating/requesting the creation or sharing/threatening to share a non-consensual sexually explicit deepfakes.

3.17 The CoE GREVIO Committee has observed that "technology can be misused by perpetrators to further intensify the coercive and controlling behaviour, manipulation and surveillance exerted on their former and current partners, therefore increasing the fear, anxiety and gradual isolation from friends and family experienced by victims".[110]

3.18 Making and sharing these images is often an attempt to control or coerce victims by using fear or shame.[111] It could be useful to clarify whether the intention to control or coerce falls within the intention to cause "humiliation, alarm or distress", or if an additional specific motive should be added. Alternatively, it could be useful to clarify whether creating or requesting the creation or sharing or threatening to share a non-consensual sexually explicit deepfake with the intention to control or coerce would be covered by the legislation on controlling and coercive behaviour (or other legislation) instead.[112]

3.19 **The NIHRC recommends that the Department of Justice clarifies whether the intention to control or coerce falls within the intention to cause 'humiliation, alarm or distress', or if an additional specific motive should be added to the proposed legislation. Alternatively, whether creating or requesting the creation, or sharing or threatening to share a non-consensual sexually explicit deepfake with the intention to control or coerce would be covered by the legislation on controlling and coercive behaviour instead.**

[109] CEDAW/C/GC/35, 'UN CEDAW Committee General Recommendation No 35: Gender-based Violence Against Women, Updating General Recommendation No 19', 26 July 2017; GREVIO(2021)20, 'CoE GREVIO Committee General Recommendation No 1: Digital Dimension of Violence Against Women' (GREVIO, 2021).
[110] GREVIO(2021)20, 'CoE GREVIO Committee General Recommendation No 1: Digital Dimension of Violence Against Women' (GREVIO, 2021).
[111] Law Commission, 'Intimate Image Abuse: A Final Report' (LC, 2022), at 87.
[112] Domestic Abuse and Civil Proceedings Act (NI) 2021.

3.20 Additionally, the offences proposed in the consultation document do not cover the perpetrator's intention to cause 'humiliation, alarm or distress' to anyone other than the person depicted in the image, such as family members or partners.

3.21 These types of images can be used for several malicious purposes, including extortion, blackmail, communications offences, controlling or coercive behaviour, harassment and stalking.[113] Perpetrators can target the person depicted in the image, as well as others close to them who may also be affected by the creation or sharing of these images.

3.22 One way to address this is to criminalise a scenario where perpetrators intend to cause distress to another person who knows, or is close to, the person depicted in the non-consensual sexually explicit deepfake. This approach should include offences related to the creation and sharing of images.

3.23 **The NIHRC recommends that the Department of Justice considers extending the offences within the proposed legislation to include scenarios where the perpetrator is targeting a person who is close to the individual depicted in the image.**

3.24 Furthermore, the offences where the motive is obtaining sexual gratification do not appear to be limited to the gratification of the perpetrator alone, but potentially the sexual gratification of others. The NIHRC welcomes this approach. However, the Department of Justice may wish to clarify if these offences relate solely to the perpetrator's gratification, or if they also include the gratification of others. Such an approach could help avoid a gap in accountability for individuals creating or sharing these images for the sexual gratification of another person.

3.25 **The NIHRC recommends that the Department of Justice specifies within the proposed legislation that offences with**

[113] Law Commission, 'Intimate Image Abuse: A Final Report' (LC, 2022), at 5; Felipe Romero Moreno, 'Generative Artificial Intelligence and Deepfakes: A Human Rights Approach to Tackling Harmful Content' (2024) 38 *International Review of Law, Computers and Technology* 297.

the motive of obtaining sexual gratification can include the perpetrator's gratification or that of other individuals.

3.26 Moreover, the offences do not seem to require proof of harm, which is something the NIHRC welcomes. Proof of harm at the reporting stages could negatively affect victims by re-victimising them and could be an evidential obstacle to prosecutions. The UN Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims are clear that "care [should be taken] to avoid… re-traumatisation".[114]

3.27 **The NIHRC recommends that the Department of Justice clarifies that the offences within the proposed legislation do not require proof of harm to protect victims from re-victimisation and excessive restrictions on prosecutions.**

Hybrid offences with specific motivations

3.28 The Department of Justice is proposing to make the offences hybrid, to broaden the range of available options to deal with different degrees of seriousness. The proposed offences require specific motivations of intention of causing humiliation, alarm or distress to the person depicted in the image, and obtaining sexual gratification.

3.29 The NIHRC welcomes that the proposed offences allow for different responses depending on the severity of the behaviour. However, the NIHRC is concerned that requiring specific intent for all offences may be overly restrictive.

3.30 The Department of Justice needs to ensure that the way the legislation is designed does not become an excessive barrier to bringing prosecutions and obtaining convictions. The Istanbul Convention is clear that legislation needs to be effective in tackling

[114] UN General Assembly, 'UN Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law', 16 December 2005, at Principle 10.

abuse and violence and bring redress for victims, particularly in cases of gender-based violence.[115]

3.31 Sometimes the creation or sharing of these images lacks a specific motivation.[116] Yet, the effects on victims can be devastating, no matter the motive.[117] Thus, it may be beneficial to add a summary-only base offence of intentionally creating or requesting the creation or sharing or threatening to share a sexually explicit deepfake without consent, or a reasonable belief in consent, regardless of motive. Such an approach may help close a potential accountability gap when the Public Prosecution Service or Police Service of NI lack evidence of a specific motive. The creation or sharing must have been intentional, so mistakes or accidents fall outside the scope of the offence.

3.32 Additionally, while this may not be needed regarding the creation of a non-consensual sexually explicit deepfake, it may be beneficial to introduce a defence of reasonable excuse to avoid over-criminalisation when sharing this type of image is necessary for reporting, preventing, detecting, investigating, or prosecuting a crime, or for the administration of justice. For example, someone might share an image to report a crime or alert the victim about its existence. Any reasonable excuse defence must be clearly defined and balanced to avoid unintentionally criminalising individuals who report crimes, while also ensuring that perpetrators remain accountable for their actions. Human rights standards emphasise the need to adopt a victim-centred approach in the development of such provisions.[118]

[115] GREVIO(2021)20, 'CoE GREVIO Committee General Recommendation No 1: Digital Dimension of Violence Against Women' (GREVIO, 2021).
[116] Law Commission, 'Intimate Image Abuse: A Final Report' (LC, 2022), at 7.
[117] Ibid.
[118] CEDAW/C/GC/35, 'UN CEDAW Committee General Recommendation No 35: Gender-based Violence Against Women, Updating General Recommendation No 19', 26 July 2017, at para 32; GREVIO(2021)20, 'CoE GREVIO Committee General Recommendation No 1: Digital Dimension of Violence Against Women' (GREVIO, 2021); UN Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power, 29 November 1985, at Principle 4; UN General Assembly, 'UN Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law', 16 December 2005, at Principle 10; CAT/C/GC/3, 'UN CAT Committee General Comment No 3: Implementation of Article 14 by States Parties', 13 December 2012, at para 21; CAT/C/GC/3, 'UN CAT Committee General Comment No 3: Implementation of Article 14 by States Parties', 13 December 2012, at paras 33, 34 and 36.

3.33 This summary-only offence would complement the more serious hybrid offences that have specific intentions behind the conduct, addressing more culpable behaviour.

3.34 Notably, there is a tiered approach in England and Wales, with strict liability offences that do not require proof of intent.[119] By comparison, the proposed approach by the Department of Justice could cause a disparity in NI regarding the protection offered to victims of non-consensual sexually explicit deepfakes. This disparity is also relevant considering this is a crime that takes place online and across jurisdictions. It raises a concern that there could be an unintended gap in protection in NI, which leads to a disproportionate approach regarding the rights of victims and people at risk, and defendants.

3.35 **The NIHRC recommends that the Department of Justice introduces within the proposed legislation a summary-only base offence of intentionally creating or requesting the creation or sharing or threatening to share a sexually explicit deepfake image without consent, or a reasonable belief in consent, regardless of motive.**

3.36 **The NIHRC recommends that the Department of Justice includes within the proposed legislation a reasonable excuse defence to avoid over-criminalisation when sharing this type of image is necessary for reporting, preventing, detecting, investigating, or prosecuting a crime, or for the administration of justice. This defence must be clearly defined and balanced, to ensure accountability without unintentionally criminalising individuals who report crimes.**

3.37 **The NIHRC recommends that the Department of Justice ensures the proposed legislation does not create an unintended gap in protection for victims in NI compared to other UK jurisdictions.**

[119] With a defence available of reasonable excuse for committing the act. See sections 66B to 66D, Sexual Offences Act 2003.

Definition of sexually explicit deepfakes

3.38 The Department of Justice is not proposing a definition of sexually explicit deepfake images for the purposes of the new offences at this point. The Department of Justice recognises that definitions need to be able to capture all aspects of this type of image and keep pace with technological advancements.

3.39 Regarding the definition of a sexually explicit deepfake, human rights standards require offences have legal certainty, including that they are clear and accessible.[120] Legal definitions (and the legal framework in general) should be clear enough to capture and keep pace with rapidly evolving artificial intelligence technology and its different uses (for example, creating, sharing, consumption, etc).[121] Thus, the definition of sexually explicit deepfake should have the capacity to respond promptly to new ways of committing these offences, and to ensuring that victims' human rights are adequately protected.

3.40 To ensure a balance between clarity and future protections, it would also be beneficial to include provisions to give the Minister the power to make regulations to include new technologies or methods of committing the offence in the legislation. An example of this power is already being proposed for the Justice Bill in relation to the review mechanism for convictions that cannot become spent.[122]

3.41 Additionally, in the new era of technological developments, it would be beneficial for the Department of Justice to explore and consider whether there are more innovative and effective ways to enable legislation to capture new technologies.[123]

---

[120] *Del Río Prada v Spain* (2013) ECHR 1004, at para 125; *Medvedyev and Others v France* (2010) ECHR 384, at para 80; CCPR/C/GC/35, 'UN Human Rights Committee General Comment No 35: Liberty and Security of Person', 16 December 2014, at para 22; *Jorgic v Germany* (2007) ECHR 583, at paras 103-114; *Kafkaris v Cyprus* (2008) ECHR 143, at para 150.

[121] GREVIO(2021)20, 'CoE GREVIO Committee General Recommendation No 1: Digital Dimension of Violence Against Women' (GREVIO, 2021).

[122] Clause 28B of the Justice Bill inserts a new Article 7A into the Rehabilitation of Offenders (NI) Order 1978 to provide the Department of Justice with a regulation-making power to allow for applications for rehabilitation in relation to sentences exceeding 10 years. See Research and Information Service, 'Briefing Paper, Justice Bill: Rehabilitation of Offenders Amendments', 30 April 2025.

[123] 'What Does a Rights-based Approach to Artificial Intelligence Look Like in NI?', JUSTICE, Law Society of NI, 22 May 2025.

3.42 **The NIHRC recommends that the Department of Justice includes a definition of sexually explicit deepfakes within the proposed legislation that is clear enough to capture and keep pace with rapidly evolving artificial intelligence technology and its different uses, with a view to ensuring that victims are adequately protected.**

Child perpetrators

3.43 The Department of Justice is proposing to qualify the application of Sex Offender notification requirements to offenders under 18 years of age, to recognise their potential effects on young people and to ensure an age-appropriate approach.[124]

3.44 The best interests of the child principle in the UN CRC requires an assessment and application of what is appropriate to the specific context and tailored to the individual circumstances of the child.[125] This includes considering the child's age, sex, level of maturity, experience, belonging to a minority group, having a physical, sensory or intellectual disability, as well as the social and cultural context in which the child or children find themselves.[126] This principle means that when dealing with child offenders, the traditional objectives of criminal justice, such as repression or retribution, must give way to rehabilitation and restorative justice objectives.[127]

3.45 The NIHRC welcomes the proposed approach. However, it would be beneficial to include express mention within the proposed legislation of the best interests of the child principle, as a primary consideration, regarding child offenders.

3.46 The Barnahus model on a child-centred approach to justice can be taken as a good practice example regarding capacity building,

[124] Ministry of Justice, 'Press Release: Increased sentencing powers for magistrates to address prisons crisis', 17 October 2024, at 20.
[125] Article 3(1) of the UN CRC requires that "in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration".
[126] CRC/C/GC/14, 'UN CRC Committee General Comment No 14: Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration", 29 May 2013, at paras 3, 32 and 48.
[127] Ibid, at para 28.

prevention, securing evidence and respecting due process in this regard.[128]

3.47 **The NIHRC recommends that the Department of Justice includes within the proposed legislation express mention of the best interests of the child principle, as a primary consideration, regarding child offenders.**

Takedowns

3.48 The Department of Justice's proposals do not include provisions that enable the removal of images from the Internet or servers.

3.49 The UN CAT Committee has specifically recommended that the UK Government and NI Executive:

> take effective measures to address low prosecution and conviction rates for domestic abuse and sexual violence in the State party, and to ensure that all cases of gender-based violence… are thoroughly investigated, that the alleged perpetrators are prosecuted and, if convicted, punished appropriately, and that the victims or their families receive redress, including adequate compensation.[129]

3.50 Generative artificial intelligence is enabling the rapid creation and distribution of sexually explicit images, reaching wider audiences with hyper-realistic quality.[130] This poses significant challenges in combating the spread of sexual abuse, particularly for victims.[131]

[128] Promise Project Series, 'Barnahus Quality Standards: Guidance for Multidisciplinary and Interagency Response to Child Victims and Witnesses of Violence' (PPS, 2017).
[129] CAT/C/GBR/CO/6, 'UN Committee against Torture Concluding Observations on the Sixth Periodic Report of the UK of Great Britain and NI', 7 June 2019, at para 57(a).
[130] Felipe Romero Moreno, 'Generative Artificial Intelligence and Deepfakes: A Human Rights Approach to Tackling Harmful Content' (2024) 38 *International Review of Law, Computers and Technology* 297; Equality Now, 'Briefing paper: Deepfake image-based sexual abuse, tech-facilitated sexual exploitation and the law' (AUDRi, 2024), at 4; Can Yavuz, 'Adverse Human Rights Impacts of Dissemination of Nonconsensual Sexual Deepfakes in the Framework of the ECHR: A Victim-Centered Perspective' (2025) 56 *Computer Law and Security Review*.
[131] Jane Wakefield, 'Tackling deepfakes "has turned into an arms race"', *BBC News*, 27 March 2024.

3.51 Despite the criminal liability for perpetrators, victims will continue to suffer harm as long as this digital content remains available online to view and share. The potential perpetual permanence and sharing of the images online can re-victimise them continuously and hugely disrupt their lives.[132] This violence can affect their family members, children, relationships, jobs, and their overall mental and physical health and life quality.[133] Thus, consideration should be given to including specific provisions that help law enforcement agencies and victims in removing this content from apps, platforms, websites, servers, and devices.

3.52 In some cases, however, removing content might be ineffective or too difficult, due to the nature of this type of sexual abuse (ease of replicating, sharing, searching and accessing this content online),[134] topped with difficulties in artificial intelligence governance and safety.[135] If efforts to remove harmful content fail in a specific case, victims should be given appropriate compensation, or alternative redress mechanisms should be established, in accordance with Articles 8 and 13 of the ECHR.[136] Article 14(1) of the UN CAT also provides that:

> each State Party shall ensure in its legal system that the victim of an act of torture obtains redress and has an enforceable right to fair and adequate compensation, including the means for as full rehabilitation as possible. In the event of the death of the victim as a result of an act of torture, his dependants shall be entitled to compensation.

[132] Adriane van der Wilk, 'Protecting Women and Girls from Violence in the Digital Age: The Relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in Addressing Online and Technology-facilitated Violence Against Women' (CoE, 2021), at 11.
[133] An EU study found that gender-based cyber harassment and stalking primarily harm women's mental health, causing anxiety, low self-esteem, depression, Post Traumatic Stress Disorder, and a lack of trust and control. Additionally, these issues lead to significant social and economic consequences, including higher healthcare and legal costs, losses in the labour market, and a reduced quality of life. This leads to the 'silencing' of women, as they withdraw from public and online spaces to protect their safety. Niombo Lomba et al, 'Combating Gender-based Violence: Cyber Violence' (EPRS, 2021), at 14.
Felipe Romero Moreno, 'Generative Artificial Intelligence and Deepfakes: A Human Rights Approach to Tackling Harmful Content' (2024) 38 *International Review of Law, Computers and Technology* 297; Can Yavuz, 'Adverse Human Rights Impacts of Dissemination of Nonconsensual Sexual Deepfakes in the Framework of the ECHR: A Victim-Centered Perspective' (2025) 56 *Computer Law and Security Review*, at 3.
[135] Hannah Brown et al, 'What Does it Mean for a Language Model to Preserve Privacy?' (ACM, 2022).
[136] *Kahn v Germany* (2016) ECHR 276, at para 75.

3.53 **The NIHRC recommends that the Department of Justice introduces specific provisions within the proposed legislation that assist law enforcement agencies and victims to remove non-consensual sexually explicit deepfakes from the internet to prevent re-victimisation.**

3.54 **The NIHRC recommends that the Department of Justice ensures there is access to adequate compensation and appropriate redress mechanisms for harm caused by the creation or sharing of non-consensual sexually explicit deepfakes, particularly when removing content is unsuccessful or ineffective.**

Specialised Training

3.55 The Department of Justice's proposals do not include provisions for specialised training. A decision may be taken that this is not for inclusion within the legislation itself, but there must be a clear plan, with committed resources in place, to ensure the necessary training is undertaken, as and when required. This is a key component of ensuring that implementation of the legislation is effective.

3.56 As best practice on this issue, Article 15 of the Istanbul Convention provides that:

> parties shall provide or strengthen appropriate training for the relevant professionals dealing with victims or perpetrators of all acts of violence covered by the scope of [the Istanbul Convention]… on the prevention and detection of such violence, equality between women and men, the needs and rights of victims, as well as on how to prevent secondary victimisation.

3.57 Specialised training is essential for successfully identifying the different types of tech-facilitated gender-based violence early and

ensuring effective responses.[137] This training should be sensitive to gender-based violence and sexual abuse, as well as to the experiences of marginalised groups such as d/Deaf and disabled persons, lesbian, gay, bisexual, transgender, queer or questioning, intersex, asexual persons, children, and persons of national or ethnic minority backgrounds. Such training should span across a victim's journey through the criminal justice system. This may require different forms of training depending on the recipient of the training, but it requires consideration of who a victim would encounter during this journey. This includes receptionists and security guards, who are often the first point of contact and are instrumental in ensuring a victim feels supported to report the crime in the first place. It also requires specialised training for professionals who may not come in contact with a victim, but would be considering their case or complaint, to ensure a victim-centred approach is adopted. Consideration should also be given to providing specialised training on a trauma-informed approach.

3.58 In addition to training, law enforcement agencies should receive additional support regarding capacity building, with a view to improving the ability to detect deepfakes and help with evidence collection. This should include adequate human, financial and technical resources to investigate and prosecute these crimes effectively.[138]

3.59 **The NIHRC recommends that the Department of Justice has a clear plan, with committed resources in place, to ensure up-to-date specialised training is available and provided as required (including refresher training) to relevant professionals and anyone who may come in contact with victims or deal with a complaint during a victim's journey through the criminal justice system. This training should be sensitive to gender-based violence and sexual abuse, as well as to the experiences of marginalised groups such as disabled persons, lesbian, gay, bisexual, transgender, queer**

[137] Adriane van der Wilk, 'Protecting Women and Girls from Violence in the Digital Age: The Relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in Addressing Online and Technology-facilitated Violence Against Women' (CoE, 2021), at 11.
[138] GREVIO(2021)20, 'CoE GREVIO Committee General Recommendation No 1: Digital Dimension of Violence Against Women' (GREVIO, 2021), at para 57.

or questioning, intersex, asexual persons, children, and persons of national or ethnic minority backgrounds.

3.60 **The NIHRC recommends that the Department of Justice ensures that there is adequate capacity within law enforcement agencies to detect deepfakes and facilitate the collection of evidence, to enable effective investigations and prosecutions.**

Education and awareness raising

3.61 The Department of Justice's proposals do not include provisions for special education and awareness-raising initiatives. Similarly, a decision may be taken that this is not for inclusion within the legislation itself, but there must be a clear plan, with committed resources in place to accommodate these.

3.62 Article 13 of the Istanbul Convention, in establishing best practice, requires States to:

> promote or conduct, on a regular basis and at all levels, awareness-raising campaigns or programmes, including in co-operation with national human rights institutions and equality bodies, civil society and non-governmental organisations, especially women's organisations, where appropriate, to increase awareness and understanding among the general public of the different manifestations of all forms of violence covered by the scope of this Convention, their consequences on children and the need to prevent such violence. Parties shall ensure the wide dissemination among the general public of information on measures available to prevent acts of violence covered by the scope of… [the Istanbul] Convention.

3.63 Education and awareness-raising initiatives should cover essential topics such as the meaning of consent, healthy relationships, and the prevention of gender-based violence. Additionally, they should

address privacy, promote non-discrimination and gender equality, and enhance digital literacy and online safety.[139] These elements are vital for creating a safer and more trustworthy digital environment. There may also be scope for a cross over with relationships and sexuality education in schools.

3.64 **The NIHRC recommends that the Department of Justice has a clear plan, with committed resources in place, for promoting education and awareness raising initiatives, focusing on prevention and encouraging reporting, the meaning of consent, healthy relationships, and the prevention of gender-based violence. It should also address privacy, promote non-discrimination and gender equality, digital literacy and online safety.**

Business and human rights

3.65 As acknowledged by the Department of Justice,[140] there is a growing artificial intelligence industry for services and products that create harmful content, almost exclusively targeting women who have not consented to its creation.[141] This non-consensual deepfake economy includes online platforms for content creation, advertisers, and credit card companies that process payments for sexually exploitative videos and images.[142] However, the Department of Justice's proposals do not include any provisions for dealing with the role of companies in enabling this type of image-based sexual abuse.

3.66 These and other artificial intelligence deployments fall within the UN Guiding Principles on Business and Human Rights, which outline the responsibilities of both States and businesses.[143]

---

[139] Ibid, at para 51.
[140] Department of Justice, 'A Consultation on Proposals to Criminalise Sexually Explicit Deepfake Images' (DoJ, 2025), at 5.
[141] Shivani Chaudhari, 'Growing demand on the dark web for AI abuse images', *BBC News*, 13 August 2024; Athena Stavrou, 'Sexual violence a 'national emergency' in UK schools amid rise of AI deepfake porn, expert warns', *The Independent*, 26 May 2025; Kat Tenbarge, 'Found through Google, bought with Visa and Mastercard: Inside the deepfake porn economy', *NBC News*, 27 March 2023.
[142] Kat Tenbarge, 'Found through Google, bought with Visa and Mastercard: Inside the deepfake porn economy', *NBC News*, 27 March 2023.
[143] A/HRC/59/53, 'UN Working Group on Business and Human Rights Artificial Intelligence Procurement and Deployment: Ensuring Alignment with the Guiding Principles on Business and Human Rights - Report of the

3.67 The UN Guiding Principles on Business and Human Rights provide a framework to prevent and address negative human rights impacts from business activities, including the use of artificial intelligence, through three pillars. These are States' duty to protect; businesses' responsibility to respect human rights, and victims' right to access an effective remedy for business-related human rights harm.[144] States must protect individuals and communities from abuses by businesses in their value chains.[145] Businesses are responsible for respecting human rights throughout the life cycle of the artificial intelligence systems they use.[146] Victims of human rights abuses related to artificial intelligence deployment by States and businesses should have access to effective remedies.[147]

3.68 Implementing all of this in practice includes ensuring the integration of a human rights-based approach into the deployment of artificial intelligence systems by businesses into their operations, products and services.

3.69 It involves requiring businesses to proactively identify risks of harm and take effective measures to address incidents, including robust content moderation and removal. Additionally, businesses should be required to cooperate with law enforcement agencies, civil society, and public authorities in NI and internationally to protect individuals from harm and prevent abuse and re-victimisation.[148]

3.70 Furthermore, introducing a ban on online platforms that primarily facilitate the creation of non-consensual sexually explicit deepfake content, such as tools marketed as 'nudifying' services, would be beneficial. When individuals have easy access to a wide range of platforms and websites that offer and promote the creation of these

Working Group on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises' (OHCHR, 2025).

[144] UN Office of the High Commissioner for Human Rights, 'Guiding Principles on Business and Human Rights: Implementing the UN "Protect, Respect and Remedy" Framework' (OHCHR, 2011).

[145] A/HRC/59/53, 'UN Working Group on Business and Human Rights Artificial Intelligence Procurement and Deployment: Ensuring Alignment with the Guiding Principles on Business and Human Rights - Report of the Working Group on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises' (OHCHR, 2025), at para 5.

[146] Ibid.

[147] Ibid.

[148] Equality Now, 'Briefing Paper: Deepfake Image-based Sexual Abuse, Tech-facilitated Sexual Exploitation and the Law' (AUDRi, 2024), at 8; Equality Now, 'Tech-facilitated Gender-based Violence'. Available at: *Tech-facilitated gender-based violence (TFGBV) | Equality Now*; GREVIO(2021)20, 'CoE GREVIO Committee General Recommendation No 1: Digital Dimension of Violence Against Women' (GREVIO, 2021), at para 55.

non-consensual images, they may naturally assume it is legal to do so. A ban would help avoid the normalisation of this phenomenon and protect people at risk of becoming victims or inadvertently committing offences.[149]

3.71 **The NIHRC recommends that the Department of Justice works with the NI Executive to ensure the integration of a human rights-based approach into the deployment of artificial intelligence systems by businesses into their operations, products and services. This includes ensuring that businesses are required to undertake robust content moderation and removal through proactively identify risks of harm, taking effective measures to address incidents, and cooperating with law enforcement agencies, civil society, and public authorities in NI and internationally to protect individuals from harm and prevent re-victimisation.**

3.72 **The NIHRC recommends that the Department of Justice introduces a ban on online platforms that primarily facilitate the creation of non-consensual sexually explicit deepfake content, such as tools marketed as 'nudifying' services to protect people at risk of becoming victims or offenders.**

[149] Rachel Hall, 'Commissioner calls for ban on apps that make deepfake nude images of children', *The Guardian*, 28 April 2025; Rachel Hall, 'What are 'nudification' apps and how would a ban in the UK work?', *The Guardian*, 28 April 2025.

Contact us

Please send any queries to Colin.Caughey@nihrc.org

www.nihrc.org | info@nihrc.org | +44 (0)28 9024 3987
4th Floor, Alfred House, 19-21 Alfred Street, Belfast, BT2 8ED