United Nations A/HRC/47/NI/2

General Assembly

Distr.: General
1 July 2021

Original: English

Human Rights Council
Forty-seventh session
21 June–9 July 2021
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Written submission by the State of the United Kingdom: Equality and Human Rights Commission (EHRC) and the Northern Ireland Human Rights Commission (NIHRC) *

Note by the Secretariat

The Secretariat of the Human Rights Council hereby transmits the communication submitted by the Equality and Human Rights Commission (EHRC) and the Northern Ireland Human Rights Commission (NIHRC)**, reproduced below in accordance with rule 7(b) of the rules of procedures described in the annex to Council resolution 5/1, according to which participation of national human rights institutions is to be based on arrangements and practices agreed upon by the Commission on Human Rights, including resolution 2005/74 of 20 April 2005.

* National human rights institution with A status accreditation from the Global Alliance of National Institutions for the Promotion and Protection of Human Rights.

** Circulated as received, in the language of submission only.

Report of the EHRC and the NIHRC following the UN Special Rapporteur on the Right to Privacy's visit to the UK in June 2018

Oversight regime for UK surveillance powers

In July 2018, the EHRC prepared a submission to the Special Rapporteur and this, as well as the End of Mission[1] statement prepared by the Special Rapporteur, highlighted the recent reform of surveillance oversight that was brought about through the passage of the Investigatory Powers Act 2016 (IPA).[2] While improved and harmonised oversight of the different aspects of the UK's surveillance regime was long overdue, EHRC and NIHRC have highlighted a number of concerns, predominantly around the compatibility of the act's bulk powers with the right to privacy.

In its briefing to the Special Rapporteur, the EHRC raised concerns regarding the IPA, including:

- Significant gaps in the requirement for judicial authorisation for some surveillance powers.

- The adequacy of safeguards for sharing intercepted material overseas.

- Whether the power to intercept and access internet connection records (weblogs) is sufficiently clear, workable in practice, and proportionate.

- Whether safeguards and oversight of the exercise of "bulk powers" are adequate to ensure they are used only where it is necessary and proportionate to do so.

A number of these topics have subsequently been the subject of domestic and regional litigation:

- In April 2018, the UK High Court found that Part 4 of the IPA, which permits bulk retention of communications data, was incompatible in certain respects with fundamental rights in EU law.[3] This was on the grounds that access to retained data was (a) not subject to prior review by a court or an independent administrative body, and (b) not limited to the purpose of combating "serious crime". [4] While amending legislation was later passed,[5] one aspect remains partially outside judicial control: the targeted acquisition and disclosure of communications data.

- In 2017, the Investigatory Powers Tribunal (IPT) referred questions to the Court of Justice of the European Union concerning the collection of bulk communications data by UK security and intelligence agencies from mobile network operators.[6] In October 2020, the Court of Justice ruled that EU law applies every time a national government forces telecommunications providers to process data, including when it is done for the purposes of national security. The court also stated that EU law sets out privacy safeguards regarding the collection of data by national governments.[7]

- On 25 May 2021, the Grand Chamber of the European Court of Human Rights (ECtHR) ruled in a case brought by multiple civil society organisations that the UK's historic

[1] UN Special Rapporteur on the Right to Privacy End of Mission Report.

[2] Investigatory Powers Act, 2016.

[3] R (National Council for Civil Liberties) v Secretary of State for the Home Department and Secretary of State for Foreign and Commonwealth Affairs [2018] EWHC 975 (Admin).

[4] Above, para. 186.

[5] Data Retention and Acquisition Regulations 2018 (SI 2018/1123) reg 1(4) read with Investigatory Powers Act 2016 (Commencement No 11) Regulations 2019 (SI 2019/174) reg 2(c), which bring IPA s. 61(1) fully into force.

[6] Privacy International v Secretary of State for Foreign and Commonwealth Affairs & Others, Order for Reference to the Court of Justice of the European Union, Case No. IPT/15/110/CH.

[7] Privacy International v Secretary of State for Foreign and Commonwealth Affairs & Others, Judgment of the Court of Justice of the European Union (Grand Chamber), Case C-623/17, 6 October 2020.

bulk intercept intelligence regime breached Articles 8 and 10 of the European Convention on Human Rights (ECHR).[8] The ECtHR emphasised the importance of 'end-to-end-safeguards' to minimise the risk of bulk interception powers being abused. Further to this, all fundamental safeguards of any Article 8 compliant bulk interception regime will now require assessment of 'necessity' and 'proportionality' at each stage of the process, independent authorisation at the outset when the object and scope of the operation are being defined, and supervision and independent ex post facto review. This ruling will help clarify the procedural safeguards that the ECHR requires to protect democracies from the increasing surveillance that technology enables. In 2019, the European Network of National Human Rights Institutions (ENNHRI) Legal Working Group, which includes the EHRC and NIHRC, submitted a third-party intervention to the ECtHR, which provided recommendations and examples of good practice as to how robust, independent and effective oversight of intelligence sharing can be guaranteed both in law and in practice.[9]

Privacy concerns in COVID-19 response

The UK Government's response to the COVID-19 pandemic has given rise to various privacy concerns,[10] including in relation to initial proposals for the NHSX contact tracing app for England to store data on a central server. However, in June 2020 the UK Government reversed these proposals and announced plans to adopt a decentralised model,[11] providing greater protection against abuse of data. In July 2020, following a legal challenge, the Department of Health and Social Care admitted to launching the NHS Test and Trace service for England without carrying out a Data Protection Impact Assessment (DPIA) addressing all aspects of the programme.[12] A DPIA was later published following the legal challenge,[13] but concerns remain about aspects of the contact tracing system.[14]

The EHRC is also concerned that safeguards in the Investigatory Powers Act 2016 have been weakened by the Coronavirus Act 2020,[15] which gave the Home Secretary the power to increase the lifespan of an urgent warrant from five to 12 working days, although such powers are time-limited.[16]

In Northern Ireland, the Children Social Care (Coronavirus) (Temporary Modification of Children's Social Care) Regulations (NI) 2020[17], extended the time period for statutory reviews and permitted the use of remote technology for visits to children in care and inspections of premises, as a response to the pandemic. The NIHRC advised both the Department of Health NI and Committee for Health on the particular need to ensure compliance with the privacy rights of children and young people during a pandemic, in order to ensure full participation in decisions affecting them.[18] The most recent proposal to extend

[8] Big Brother Watch and Others v the United Kingdom (Grand Chamber), Application Nos. 58170/13, 62322/14, 24960/15, 25 May 2021.

[9] Big Brother Watch and Others v the United Kingdom, Application Nos. 58170/13, 62322/14 and 24960/15, Written submissions of the European Network of National Human Rights Institutions, 26 April 2019.

[10] Joint Committee on Human Rights (2020), Human Rights and the Government's Response to Covid-19: Digital Contact Tracing.

[11] Department of Health and Social Care (2020), Health and Social Care Secretary's statement on coronavirus (COVID-19): 18 June 2020; Department of Health and Social Care (2020), Breaking chains of COVID-19 transmission to help people return to more normal lives: developing the NHS Test and Trace service.

[12] Government Legal Department (2020), Letter RE: Open Rights Group and the NHS Test & Trace Programme.

[13] Department of Health and Social Care (2020), NHS COVID-19 app: privacy information.

[14] Joint Committee on Human Rights (2020), The Government's response to COVID-19: human rights implications, p.50-52.

[15] Coronavirus Act 2020, sections 22 and 23.

[16] The Investigatory Powers (Temporary Judicial Commissioners and Modification of Time Limits) Regulations 2020.

[17] Children Social Care (Coronavirus) (Temporary Modification of Children's Social Care) Regulations (NI) 2020.

[18] NIHRC, 'Submission on the Children Social Care (Coronavirus) (Temporary Modification of Children's Social Care) Regulations (NI) 2020', May 2020.

was withdrawn following continuing concerns from the NIHRC, and other NGOs, about the privacy of children and young people.

Policing, data retention, and facial recognition technology

Following EHRC's submission to the UN Special Rapporteur on the Right to Privacy, the ECtHR has ruled on *Catt v the United Kingdom.*[19] The ECtHR found that the UK Government violated the right to privacy (Article 8 ECHR) of the applicant and while there was a pressing need to collect the personal data about the applicant, there was no pressing need to retain it. The ruling called for increased safeguards for personal data collected overtly by the police. The ECtHR also noted that the absence of effective safeguards was of particular concern in relation to personal information about political opinions, where retention could have a 'chilling effect' on the right to engage in peaceful protest.

The use of automated facial recognition in policing, and its impact on privacy rights, has become an increasing concern in recent years. In August 2020, the Court of Appeal found that there were 'fundamental deficiencies' in the legal framework governing the use of automated facial recognition, and that its use was in breach of the right to privacy (Article 8 ECHR), the Data Protection Act 2018 and the Public Sector Equality Duty.[20] The Information Commissioner's Office (ICO) has previously stated[21] that data protection law sets high standards in relation to the use of Live Facial Recognition (LFR) in a law enforcement context and when used in public places. Furthermore, in its latest opinion,[22] the ICO highlights the concern that "LFR systems may also work less effectively for people from different demographic groups. This could potentially lead to unfairness in the form of discrimination and bias."

Northern Ireland: Biometric retention and legacy issues

Due to political disagreement on the application for legacy investigations, legislation to give effect to the ECtHR judgment of *S and Marper v the United Kingdom*[23] was passed by the NI Assembly but never commenced in NI.[24] The NIHRC initiated legal action against the Police Service of NI (PSNI) in respect of its interim arrangements for the retention and disposal of DNA and fingerprints. This case was settled by way of an agreement to produce an ECHR compliant process in the absence of political agreement. A draft was produced by PSNI with input from NIHRC and an agreement was reached in principle to destroy significant amounts of biometric material. This process has been overtaken by the ECtHR judgment in *Gaughran v the United Kingdom*, which held that the policy of indefinite retention, without reference to the seriousness or the offence and in the absence of the possibility of review, was a disproportionate interference with the right to privacy (Article 8 ECHR).[25] With a view to addressing this finding, the Department of Justice NI has consulted on proposals to amend the legislation; proposing an end to indefinite retention and instead using the 75, 50 and 25 year model for retaining DNA and fingerprints of convicted individuals. It has also proposed that this new approach would include a review system that would be put in regulations, which has yet to be published. The NIHRC has continuing concerns that even revised proposals are too broad and disproportionate in terms of the balance between interference with Article 8 and the protection of the public.[26] Separate and more wide-ranging arrangements are made to retain biometric material for the purposes of legacy investigations.

---

19 Catt v the United Kingdom, Application no. 43514/15, 24 January 2019.

20 Bridges v South Wales Police, Court of Appeal, Case No: C1/2019/2670, 11 August 2020.

21 Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places, 31 October 2019.

22 Information Commissioner's Opinion: The use of live facial recognition technology in public places, 18 June 2021.

23 S and Marper v the United Kingdom, Application no. 30562/04 and 30566/04, 4 December 2008.

24 Criminal Justice Act (NI) 2013.

25 Gaughran v the United Kingdom, Application no 45245/15, 13 June 2020.

26 NIHRC, 'Submission to to DoJ Consultation on Proposals to Amend the Legislation Governing the Retention of DNA and Fingerprints in NI', September 2020; NIHRC, 'Submission to the Committee for Justice on Proposals to Amend the Legislation Governing the Retention of DNA and Fingerprints in Northern Ireland – Outcome of Consultation and Proposed Way Forward', 14 December 2020.

The implications of biometric retention on legacy investigations has also been highlighted by the NIHRC to the Committee of Ministers, in response to the action plan provided by the UK Government that suggested that the Data Protection Act 2018 and the oversight of the Information Commissioner's Office has addressed the issue for both legacy and non-legacy investigations. As a result, no further legislative reform was necessary elsewhere in the UK.[27] On legacy investigations, the NIHRC remains concerned at the ongoing failure of the UK Government to introduce legislation regarding the investigation of conflict-related deaths, and Article 3 ECHR (prohibition of torture) cases. Legislation to address these mechanisms was anticipated following an extensive consultation process on a draft Bill. However, after a roll back on commitments in March 2020, no further progress has been made[28]. Indeed, the issue of wider retention of biometric material is currently dealt with by way of transitional legislation permitting the continued retention of data under counter-terrorism powers, first introduced in 2013 and renewed periodically, most recently in 2020 for another two years.[29]

[27] NIHRC, 'Submission to the Committee of Ministers in Relation to the Supervision of the Cases Concerning the Actions of the Security Forces in Northern Ireland', May 2020.

[28] Written Ministerial Statement, 'Addressing Northern Ireland Legacy Issues' 18 March 2020.

[29] The Protection of Freedoms Act 2012 (Destruction, Retention and Use of Biometric Data) (Transitional, Transitory and Saving Provisions) (Amendment) Order 2020.