Submission to Joint Committee on Justice, Home Affairs and Migration

General Scheme of the National Cyber Security Bill 2024

Digital Rights Ireland and the Irish Council for Civil Liberties

August 2025

1. Summary

1.1 Digital Rights Ireland (DRI) and the Irish Council for Civil Liberties (ICCL) thank the Committee for the opportunity to make submissions on the General Scheme of the Bill.

1.2 In these submissions we cover some aspects of the Heads of Bill which go beyond the requirements of the second Network and Information Security Directive[1] (NIS2) and therefore are not required for transposition of NIS2 into Irish law.

1.3 In evaluating these provisions it must be remembered that the National Cyber Security Centre (NCSC) is not an independent body. Head 3 explicitly provides that it is 'under the authority of the Minister'. This is particularly important in relation to the rights to privacy and data protection under Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the Charter of Fundamental Rights. As a rule, those instruments require independent authorisation of surveillance to prevent misuse and politicisation of surveillance powers.[2]

2. Head 6 – Scanning

2.1 This Head would permit the NCSC to scan any publicly accessible network or information system in the State for vulnerabilities, without notifying the owner or seeking their consent. This goes beyond the requirements of NIS2, which requires CSIRTs to have powers to scan essential or important entities only,[3] and would allow the NCSC to

[1] Directive (EU) 2022/2555.
[2] See e.g. TJ McIntyre, 'Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective' in Martin Scheinin, Helle Krunke and Marina Aksenova (eds), *Judges as Guardians of Constitutionalism and Human Rights* (Edward Elgar 2016).
[3] NIS2, Article 11(3).

scan networks belonging to e.g. small businesses, political parties, or even home networks. The Explanatory Note does not justify the expansion of this power, and there is no requirement that it be exercised based on an assessment of necessity or proportionality. We recommend that this be amended to provide that the NCSC may scan networks only with the consent of the relevant entity, except in relation to essential or important entities.

2.2 Alternatively, if the aim behind this Head is in fact to permit widespread scanning (for example, to detect compromised devices such as video doorbells or routers on private networks) then it should be redrafted to make this clear, to require independent authorisation of such scanning based on explicit criteria, and to explain how such scanning would be subject to safeguards to ensure that it is limited to what is necessary and proportionate.

3. Head 7 – DNS blocking and sinkholing

3.1 Head 7 is of particular importance given the wide and uncertain scope of the powers it would create. While the title refers to 'DNS blocking and sinkholing', Head 7(2) goes significantly further by referring to 'appropriate measures' to be taken by both DNS providers and domain registrars. As written, this seems to go beyond DNS blocking and sinkholing (broadly speaking, causing DNS look up requests for a domain name to resolve to a different IP address or to a non-routable IP address) and would also include suspension or revocation of a domain name.

3.2 The significance of these measures lies in the way in which they can act as an internet death penalty for a particular domain name. Simply put, if DNS providers in Ireland (typically an individual's broadband provider) suspends a domain name then this will have the effect of cutting off access to any websites or other material hosted on that domain name.[4] DNS blocking is also extremely likely to cause overblocking by cutting off access to unrelated material which happens to be hosted on the same domain name, affecting third party rights also.[5]

[4] Except for users with the knowledge to use a virtual private network (VPN) or to use a different DNS resolver.

[5] See e.g. Richard Clayton, 'Failures in a Hybrid Content Blocking System' (Workshop on Privacy Enhancing Technologies, Dubrovnik, 30 June 2005) <http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf> accessed 17 April 2009; Cormac Callanan and others, *Internet Blocking: Balancing Cybercrime Responses in Democratic Societies* (Aconite Internet Solutions 2009) <http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf>; TJ McIntyre, 'Child Abuse Images and Cleanfeeds: Assessing Internet Blocking Systems' in Ian Brown (ed), *Research Handbook on Governance of the Internet* (Edward Elgar 2013).

3.3 DNS blocking and domain name suspension therefore raise significant issues for the right to freedom of expression, as well the rights of businesses who may find their websites inaccessible through no fault of their own. The Committee of Ministers of the Council of Europe in the 2018 *Recommendation on The Roles and Responsibilities of Internet Intermediaries* has recommended that measures of this sort should take place only subject to the following safeguards:

> 1.3.2. State authorities should obtain an order by a judicial authority or other independent administrative authority, whose decisions are subject to judicial review, when demanding intermediaries to restrict access to content. This does not apply in cases concerning content that is illegal irrespective of context, such as content involving child sexual abuse material, or in cases where expedited measures are required in accordance with the conditions prescribed in Article 10 of the Convention.
>
> 1.3.3. When internet intermediaries restrict access to third-party content based on a State order, State authorities should ensure that effective redress mechanisms are made available and adhere to applicable procedural safeguards…
>
> 2.3.3. Any restriction of content should be limited in scope to the precise remit of the order or request and should be accompanied by information to the public, explaining which content has been restricted and on what legal basis. Notice should also be given to the user and other affected parties, unless this interferes with ongoing law-enforcement activities, including information on procedural safeguards, opportunities for adversarial procedures for both parties as appropriate and available redress mechanisms.[6]

3.4 It is clear, however, that Head 7 does not address these requirements.

3.5 It is also important to point out that NIS2 does not require that the NCSC be given blocking powers. The Explanatory Note to Head 7 is somewhat misleading on this point. The Explanatory Note says 'In Recital 126 of NIS2, it states that in duly substantiated cases where it is aware of a significant cyber threat or an imminent risk, the competent authority should be able to take immediate enforcement decisions with the aim of preventing or responding to an incident.' However Recital 126 refers to 'enforcement decisions' using the powers set out in NIS2 itself – not any other national powers.

[6] Committee of Ministers of the Council of Europe, 'Recommendation CM/Rec(2018)2 on the Roles and Responsibilities of Internet Intermediaries' (2018) <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14> accessed 15 October 2019.

3.6 Finally, we should also point out some drafting issues with Head 7. Head 7(1) refers to a 'National Security' threat, but this term does not appear to be defined elsewhere in the Heads of Bill and there is no general definition of 'national security' in Irish law. In addition, it is not clear whether Head 7 creates a compulsory power or merely a power to request that a provider consider action. Head 7(2) states that the NCSC may 'ask a DNS Service Provider or domain register to take appropriate measures to this threat [*sic*]', while Head 7(4) states that the NCSC 'may request a domain name resolution system operator, to take such actions as required to terminate the DNS abuse.' If these are in fact intended to create compulsory powers then the language used ('appropriate measures' and 'such actions as required') would be too vague to have binding effect.

3.7 We therefore recommend that Head 7 be withdrawn, and that any measure regarding blocking or domain name suspension be redrafted in accordance with the requirements of the European Convention on Human Rights.

4. Head 8 - Sensor Employment on Networks of Essential and Important Entities

4.1 It is difficult to overstate how privacy invasive this provision would be. In concrete terms, it would permit the NCSC to collect the entirety of the network traffic in public sector bodies (including, for example, sensitive health data in hospitals and the contents of emails to/from legal advisers), as well as all metadata about private communications carried on public electronic communications networks (such as mobile phone and home broadband providers) and private communications carried on social network providers. This information could then be stored for up to 18 months.

4.2 While Head 8 requires the consent of the 'entities concerned', this is not the same as the consent of the individuals affected. Head 8 enables bulk collection of data relating to all employees, visitors, users and even Irish residents in general, and information not limited to suspected threats but potentially covering all communications on a network.

4.3 There is no requirement in Head 8 that the use of such a system be proportionate. Head 8(2) provides that this data may be collected 'to the extent strictly necessary for the detection and management of threat and risks to network and information security', but does not include any limitation to serious or significant threats or risks.

4.3 Such a far reaching power would be contrary to the requirements of Article 8 of the European Convention on Human Rights as well as the requirements of the GDPR[7] and the ePrivacy Directive.[8]

4.4 In relation to metadata, there is an extensive line of caselaw from the Court of Justice of the European Union (CJEU), starting with the judgment in *Digital Rights Ireland,* which precludes the general and indiscriminate retention of communications traffic and location data for the purposes of policing criminal behaviour, and provides that access to such data must be based on a prior review carried out by a court or independent administrative authority.[9] Under Head 8 there would be no independent authorisation of any sort.

4.5 The collection of the content of communications is more invasive still, and the CJEU has held in *Schrems I* that 'legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter'.[10]

4.6 Head 8(3) appears to create a purpose limitation principle in relation to this data, by stating that 'Individually designated and specially authorised officials of the NCSC shall be authorised, for the sole purpose of preventing and characterising the threat affecting the information systems of the entities referred to in the first subparagraph of this article, to collect data and analyse only the relevant technical data, to the exclusion of any other exploitation.' However, this provision is undermined subsequently by Head 10(1) which permits processing of personal data for purposes other than those for which the data was collected, and by Head 11 which permits information sharing with the Garda Síochána.

4.7 We recommend that this Head be redrafted to limit it to significant threats or risks, to limit the retention of data to that which is both necessary and proportionate to such risks, and to limit the retained data to metadata only unless it is shown that it is necessary to retain a particular category of content data (such as files containing particular forms of

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC..
[8] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
[9] See in particular Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and others* [2014] ECLI:EU:C:2014:238; Joined Cases C-203/15 and C-698/15, *Tele2 Sverige and others* [2018] ECLI:EU:C:2016:970; Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others* [2020] ECLI:EU:C:2020:791; Case C-140/20, *G.D. v. Garda Commissioner* [2022] ECLI:EU:C:2022:258.
[10] Case C-362/14, *Schrems* [2015] ECLI:EU:C:2015:650, para. 94.

malware), in which case the retention of content data should be limited to that category of data.

5. Head 9 - Temporary Sensor Employment on Communications Networks

5.1 This Head raises similar concerns to Head 8, exacerbated by the fact that it creates a compulsory surveillance power which can extend to the telephony and internet use of the entire population.

5.2 For the most part Head 9 is structurally an extension of the existing data retention scheme established under the Communications (Retention of Data) Act 2011.[11] However, it goes considerably further in two regards. First, the 2011 Act applies, essentially, only to traditional telephony and broadband providers.[12] However Head 10 would also apply to over the top communication services (such as WhatsApp) and data centre operators also. Second, the 2011 Act merely permits state bodies to seek data from providers. Head 9, however, is considerably more invasive in that it can require providers to install surveillance devices on their networks, restricting their ability to monitor or challenge state surveillance.

5.3 As already discussed, there is now an extensive jurisprudence of the CJEU setting out the circumstances in which general and indiscriminate data retention is permissible. In relation to national security, the CJEU has held that this type of data retention may be used only:

> 'where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists'.[13]

5.4 However, Head 9 does not meet the requirements of that jurisprudence. Head 9(1) refers to a 'pressing National Security threat', which as discussed is not a term recognised under Irish law. Head 9(8) then sets the criteria for use of these powers as being that 'the

[11] As amended.
[12] TJ McIntyre and Maria Helen Murphy, 'Accessing Digital Evidence in Criminal Matters: An Inadequate Irish Legal Framework' in Vanessa Franssen and Stanisław Tosza (eds), *The Cambridge Handbook of Digital Evidence in Criminal Investigation* (Cambridge University Press 2025).
[13] Case C-140/20, *G.D. v. Garda Commissioner* [2022] ECLI:EU:C:2022:258, para. 58.

NCSC has grounds for believing that there are real and present risks to the security of the State or the confidentiality, integrity or authenticity of public sector data or to the continuity of Essential Services'. This, however, falls short of the CJEU requirement that there be a 'serious threat to national security' and instead equates all risks to public sector data with serious national security risks. Most fundamentally, it does not provide that the use of these mass surveillance powers should be proportionate to the threat.

6. Head 10 - Processing of Personal Data

6.1 Overall, the provisions of Head 10 appear unclear, imprecise and unforeseeable. As such they risk leading to a disproportionate interference with individuals' fundamental rights to privacy and data protection.

6.2 Head 10's reliance on broad justifications to process personal data, for purposes other than those for which the data were originally collected, such as 'to collect, evaluate or investigate information on security risks or security precautions', 'for support, advice or warning in questions of security' and 'for reasons of national security' lacks definitional boundaries or procedural safeguards, making it difficult for individuals to foresee how their data might be processed. Laws enabling indiscriminate data access or processing without clear limits or oversight risk being found to have breached the principles of necessity and proportionality.

6.3 Of particular concern is Head 10(2)(b) which gives the NCSC permission to process special category data where excluding such data would 'make the fulfilment of the tasks of the NCSC impossible or significantly endanger them.' This wording is overly broad and insufficiently defined, risking unjustified processing of people's highly sensitive personal data.

6.4 Article 9(2)(g) GDPR provides that processing of special category data can occur 'if necessary for reasons of substantial public interest' but such processing requires that the law providing for such processing be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard people's fundamental rights. These specific conditions and safeguards are entirely absent from this Head.