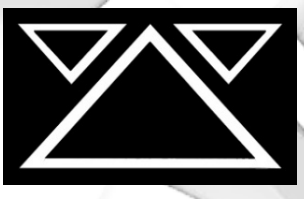
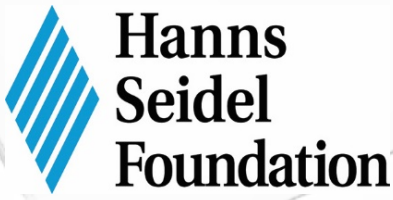
Communications Act 8 of 2009: Is the collection and retention of data on telecommunications users constitutional?



Legal Assistance Centre

Windhoek | Namibia

June 2021



Legal Assistance Centre (LAC)

Street address:
4 Marien Ngouabi Street, Windhoek

Postal address:
P.O. Box 604, Windhoek, Namibia

Telephone:
(+264) 061-223356

Fax:
(+264) 061-234953

Email:
info@lac.org.na

Website:
www.lac.org.na

Facebook:
https://www.facebook.com/LACNamibia/

1. Introduction

1.1 What is data retention?

Telecommunications networks collect and generate an enormous amount of data that can reveal the identity of users as well as detailed profiles of their communications activity. An increasing number of States are enacting laws that require the retention and organisation of such data for later access by law enforcement officials who are carrying out specific investigations. The theory is that this kind of data can be very helpful in preventing and combating crime, particularly in areas such as child pornography, organised crime and terrorism. Opponents of such schemes point to the widespread invasion of privacy involved, as well as the potential abuse for unjustified State surveillance and the danger that such a treasure trove of data will be hacked by unauthorised persons and used for purposes such as identity theft or corporate marketing.[1]

Namibia is about to join the ranks of States that mandate the retention of data about all telecommunications users, when additional parts of the Communications Act 8 of 2009 come into force – as is expected to take place soon.

The question under consideration is whether Namibia's requirements for telecommunications data collection and retention might be unconstitutional. Since Namibia has virtually no jurisprudence on the constitutional right to privacy as yet, this memo focuses on key European Union cases and findings of unconstitutionality in India and South Africa.[2]

2. Namibia

2.1 Namibian legal requirements

Communications Act, section 73

Namibia's Communications Act 8 of 2009[3] contains a provision that requires telecommunications service providers to collect and retain certain information about their customers:

> **Duty to obtain information relating to customers**
>
> **73.** (1) Telecommunications service providers must ensure that the prescribed information is obtained from all customers.
>
> (2) The information referred to in subsection (1) must be sufficient to determine which telephone number or other identification has been issued to a specific customer in order to make it possible to intercept the telecommunications of that customer.

The Act defines **"customer"** as follows:

> "customer" means any person who concluded a contract with the provider of telecommunications services for the provision of such services;

It defines **"telecommunications services"** as follows:

> "telecommunications services" means services whose provision consists wholly or partly in the transmission or routing of information on telecommunications networks by means of telecommunications processes but does not include broadcast services;

---

[1] For a general introduction to the practice that focuses on its risks, see "Introduction To Data Retention Mandates", Center for Democracy & Technology, September 2012, https://cdt.org/wp-content/uploads/pdfs/CDT_Data_Retention-Five_Pager.pdf.

[2] Throughout the report, boldface type is not present in the original texts quoted but has been added for emphasis by the author.

[3] This Act was was brought into force, with the exception of Parts 4 and 6 of Chapter V (universal service and interception of telecommunications) and Chapter IX (establishment and incorporation of .na domain name association), on 18 May 2011. Part 4 of Chapter V (universal service) was brought into force on 1 December 2016. The remaining provisions will come into force on a date or dates set by the Minister by notice in the *Government Gazette.*

New Namibian regulations on data retention

Section 73 of the Communications Act has not yet been brought into force, but regulations to facilitate its application have already been issued in preparation for its enactment.[4] These regulations, which were issued in March 2021, provide **details about the duty of telecommunications service providers to collect and retain certain information about their "customers".**

The regulations contain a more detailed definition of **"customer"** than the one provided in the Act:

> "customer", in relation to a service provider, means a person with whom a service provider has concluded a contract to provide a telecommunications service and if the service provider does not belong to a class of persons excluded by regulation 2(2) or regulation 2(3) and "customer" includes a prospective customer.

The **excluded persons under regulation 2(2)** are persons who provide telecommunications services as an incidental part of another business, by providing access to the internet or other telecommunications services to their customers or to people present on their premises, or those who allows their customers or their customers' guests to use telecommunications services obtained from a different service provider. This would apply, for instance, to internet services provided at places such as coffee shops, restaurants and hotels.

The **excluded persons under regulation 2(3)** are persons who operate an electronic network for their own purposes and allow employees or other persons to access the internet or other telecommunications services through that network. This would appear to cover businesses that provide telecommunications services through their own servers.

The wording of the definitions of "customer" in both the Act and the regulations appears to *exclude* the use of pre-paid cell phone services, due to the reference to a "contract".

The regulations specifically indicate that the term "customers" does include "foreign nationals" (reg 7(1)).

Regulation 7(5) and (6) list the information that a telecommunications service provider must obtain from a customer before providing services to that customer.

> For customers who are **natural persons**:
>
> (a) the **full name** of the customer;
> (b) the **address** at which the customer ordinarily resides or if the customer ordinarily resides outside Namibia, the address at which the customer resides while he or she is in Namibia and the address at which the customer works or from which he or she conducts his or her business;
> (c) a **Namibian identity number** or, if the customer in question does not have a Namibian identity number, the number of the document referred to in paragraph (d);

---

[4] *Regulations in terms of Part 6 of Chapter V* were issued in terms of section 77 of the Act in GN 40/2021 (GG 7481) dated 15 March 2021. Note that it appears to be competent for the Ministry to publish regulations as preparation for bringing this portion of the law into force, but the regulations published in this way may *not* come into force before the relevant portion of the Act is brought into force. See section 12(3) of the Interpretation of Laws Proclamation 37 of 1920:

> (3) Where a law confers a power -
> ...
> (b) to make, grant, or issue any… regulations...
> …
>
> that power may, unless the contrary intention appears, be exercised at any time after the passing of the law so far as may be necessary for the purpose of bringing the law into operation at the commencement thereof, subject to this restriction that any ... regulations... made... under the power shall not, unless the contrary intention appears in the law or the contrary is necessary for bringing the law into operation, come into operation until the law comes into operation.

This issue is discussed in *Minister of Health and Social Services & Others v Medical Association of Namibia Ltd & Another* 2012 (2) NR 566 (SC) at paras 63-69.

(d) a copy of -
  (i) any **identity document** containing a recent photograph of him or her issued under any law governing the identification of persons in Namibia or any such official document of identity issued by the government of any other country;
  (ii) if the customer ordinarily resides outside Namibia or does not have a document referred to in subparagraph (i), a **passport** issued to the customer;
  (iii) if the customer in question does not have a document referred to in subparagraph(i) or (ii), a **driving licence or permit containing a recent photograph** of him or her, whether issued in or outside Namibia.

For customers who are **juristic persons** such as companies or voluntary associations:

(a) the **information referred to in subregulation (5) of the natural person representing the juristic person** in the conclusion of the contract with the service provider as well as that information of the natural person who will be using the service on behalf of the juristic person or if the service is not being used by a specific natural person, a statement of that fact and an explanation of the purpose of the service;
(b) the **full name of the juristic person**;
(c) the **registration number of the juristic person**, if any;
(d) the **business address** of the juristic person;
(e) a copy of a **letter on the letterhead of the juristic person specifying that the person representing the juristic person has the authority to represent the juristic person** in the conclusion of a contract with a service provider to provide telecommunications services.

The collection of the listed information applies to **new customers** three months after the underlying legal provision comes into force (reg 7(1)), while there is a grace period of 12 months after that date for collecting the information from **existing customers** (reg 10(1)) – and **telecommunications services for any customer must be cancelled if the information is not provided after the prescribed warnings have been given to the customer** (reg10(2)-(7)).

The service provider must store the listed identifying information with reference to the customer's full name and surname to facilitate retrieval (reg 7(7)), and it must retain the information for at least **five years** following the cancellation of the relevant contract along with the telephone number or other identification provided to the customer under the contract (reg 7(8)).

There is an **exemption** from the data retention requirement where the telecommunications services are provided by a Namibian service provider in terms of an agreement with a **foreign service provider** (reg 7(9)) – in other words, where the Namibian service provider is a customer of a foreign service provider that is actually providing the services.

The customer must complete a form containing the required identifying information and certifying that it is correct. It is a criminal offence to provide false information on this form (reg 8). The same rules apply if the "form" is digital instead of paper-based (reg 9).

Regulation 3(1) lists additional information that telecommunications service providers must collect and store for at least five years in respect of their customers ("insofar as the information is applicable to the form of telecommunications services in question"):

(a) the **telephone number** or **other identification** of the customer concerned;
(b) the **internet protocol address** allocated to a customer (irrespective of whether that address is allocated only for the duration of a telecommunications session or whether it is allocated permanently to a specific customer) **in addition to any information that might be necessary to link a specific packet to a specific customer**;
(c) the **called number** if the call is generated by the user of the service of the service provider and the **calling number** if the call is initiated by another party than the user of the service of the service provider;
(d) the **source and destination of any other telecommunications** in a form that is appropriate for the protocol or application in question: Provided that when a packet based protocol is used, it is not necessary to store the data relating to every packet, as long as a summary containing the total amount of data transferred and the source and destination of the transfer, is stored;

(e) the **date, time and duration of the telecommunications**;
(f) **particulars similar to the information referred to in this subregulation relating to supplementary services or facilities** used in association with the telecommunications such as multi-party conferencing, call diversion, abbreviated dialing [sic] and voice mail;
(g) **intermediate numbers** where the customer establishes conference calling or calls to link through services;
(h) identification of **base station and cell site**, in respect of all cellular phones or similar devices in such detail and at such resolution as is normally required to render an efficient service; and
(i) the **nature of the telecommunications** whether it is voice, fax, a message service or any other form of data.

The service provider must store the listed information in a manner that allows retrieval in terms of the regulations or any other law authorising the interception of telecommunications or requiring "the provision of information relating to telecommunications to another institution" (reg 3(2)).

Under regulation 5, **information from the stored data about a specific person can be requested by a member of the Namibian Police Force or a staff member of the Namibia Central Intelligence Service, after getting authority from a judge or a magistrate.** This application requires a statement of

- the **offence** being investigated (police) or the **reasons** for the request (intelligence services);
- the **specific person whose information is required**;
- a **specific description of what information is being requested**; and
- a **statement under oath giving reasons why the required information is necessary or relevant for the investigation concerned and why it is not expedient to obtain the information in any other manner**.

The word "person" appears in the singular, suggesting that separate applications are required for information about multiple individuals.

The judge or magistrate can grant the application only after being satisfied on three points: (1) that the **requested information is "necessary or relevant" for the investigation** concerned; (2) that there is **"no other expedient manner of obtaining the information concerned"**; and (3) that "**the obtaining of the information is authorised by the law of Namibia"**.

As is the usual case with similar laws on search warrants, **the regulations make provision for the police (but not the intelligence services) to access customer information from a telecommunications service provider *without court authorisation* in urgent situations. However, the approach of this provision is odd because it places the decision-making burden on the *telecommunications service provider* instead of on the trained police officer.** The regulations require the police officer making the request to convince the *authorised officer at the telecommunications service provider* "on reasonable grounds" of three things: (1) that the requested information is required urgently; (2) that the delay in getting court authorisation would defeat the purpose of the request; and (3) that a request to the court for authority for requesting the information would have been granted if it had been made (reg 5(7)). In contrast, in terms of the Criminal Procedure Act 51 of 1977, it is the police officer who must make that assessment.[5]

This approach presents several problems. Firstly, service providers designate the staff members who will function as "authorised staff members", and they can be selected individually or identified on the basis of the positions that they hold. The names/positions must be provided to the Communications Regulatory Authority of Namibia, but there are no requirements concerning qualifications, training or even orientation to the relevant law. The selection of these persons/positions is solely at the discretion of the service provider (reg 4). This means that the "authorised staff members" of telecommunications service providers are unlikely to have training or experience in legal matters. Secondly, a police officer is subject to statutory authority and could be disciplined

[5] **22.** A police official may without a search warrant search any person or container or premises for the purpose of seizing any article referred to in section 20 -
(a) if the person concerned consents to the search for and the seizure of the article in question, or if the person who may consent to the search of the container or premises consents to such search and the seizure of the article in question; or
(b) if he [the police official] on reasonable grounds believes -
(i) that a search warrant will be issued to him under paragraph (a) of section 21 (1) if he applies for such warrant; and
(ii) that the delay in obtaining such warrant would defeat the object of the search.

if he or she abused the power to bypass judicial authorisation to access information – but there would no similar recourse against staff members of a private telecommunications service provider.

The regulations make provision for **modest payments to telecommunications service providers in respect of each "interception target" and each information request**, as well as amounts to cover printing costs and electronic copying costs and overtime work required to respond to requests for data or interceptions (reg 6).

2.2 Jurisprudence on Namibia's constitutional right to privacy

Article 13 of the Namibian Constitution covers the protection of privacy, which is the constitutional right most closely implicated by the regulatory scheme described.

> **Article 13 Privacy**
> (1) No persons shall be subject to interference with the privacy of their homes, correspondence or communications save as in accordance with law and as is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.
> (2) Searches of the person or the homes of individuals shall only be justified:
> (a) where these are authorised by a competent judicial officer;
> (b) in cases where delay in obtaining such judicial authority carries with it the danger of prejudicing the objects of the search or the public interest, and such procedures as are prescribed by Act of Parliament to preclude abuse are properly satisfied.

The constitutional right to privacy has been raised in support of cases seeking to invalidate portions of several statutes and one aspect of the common-law – but most of these cases have been decided on other grounds, and none contains any detailed judicial analysis of the right to privacy.

(1) In 1998, the High Court considered provisions in the **Indecent and Obscene Photographic Matter Act, 37 of 1967** that prohibited the sale of "indecent or obscene photographic matter" as well as the sale of adult toys and novelties intended for use "to perform unnatural sexual acts" in violation of the **Combating of Immoral Practices Act 21 of 1980**. It was alleged that these provisions impermissibly violated the constitutional right to privacy, but the Court stated that the constitutional rights more directly implicated were the right to freedom of speech and expression and the freedom to carry on any trade or business. It found that the restrictions contained in the statutes in questions were overly broad mechanisms for achieving the State objective of upholding standards of decency and morality in society.[6]

(2) In 2002, the High Court considered several provisions of the **Combating of Immoral Practices Act 21 of 1980** relating to prostitution. The right to privacy was raised, but the Court found that the only constitutional right infringed was the right to practise any profession, or carry on any occupation, trade or business. It found that, while the law's objective to maintain and promote public order, decency and morality was permissible, some of the expressions of prohibited activities were excessively sweeping and vague, thus going beyond restrictions that are reasonably required for the realisation of the Act's objectives – and thus falling short of the minimum impairment rule and the requirement that limitations on a constitutional right must be proportional to the interests the Act is seeking to protect.[7]

(3) The Supreme Court, in the process of ruling that the **delict of adultery** has no further place in Namibian law, found that actions seeking damages for adulterous behaviour are incompatible with a number of constitutional values, including privacy – but without elaborating on the right to privacy:

---

[6] *Fantasy Enterprises CC t/a Hustler The Shop v Minister of Home Affairs; Nasilowski v Minister of Justice* 1998 NR 96 (HC).

[7] *Hendricks v Attorney-General Namibia* 2002 NR 353 (HC).

> But ultimately, it is in respect of the determination of wrongfulness — with reference to the legal convictions of the community informed by our constitutional values and norms — that it is no longer reasonable to impose delictual liability for a claim founded on adultery. Whilst the changing societal norms are represented by a softening in the attitude towards adultery, **the action is incompatible with the constitutional values of equality of men and women in marriage and rights to freedom and security of the person, privacy and freedom of association**. Its patriarchal origin perpetuated in the form of the damages to be awarded is furthermore not compatible with our constitutional values of equality in marriage and human dignity.[8]

Another line of cases has taken the view that laws which provide justifiable interference with the right to privacy – by providing for searches and seizures or access to personal information – must be strictly construed and correctly applied.

(1) In 2019, the High Court considered a case where **the procedure for obtaining information in terms of the Anti-Corruption Act 8 of 2003 had not been properly followed**. The Court ruled that the legal procedures provided by the law must be strictly followed to avoid an inappropriate infringement of privacy, and held that the evidence obtained without following the prescribed procedures was inadmissible.[9] The crux of the Court's reasoning appears from the excerpt below:

> Article 13 of the Namibian Constitution deals with the fundamental right of privacy… In terms of this article the right to privacy of a person is not absolute and may be interfered with by law ie by Act of Parliament. One such instance is s 27(1) of the [Anti-Corruption] Act where the ACC obtains access to a person's bank account which otherwise would have been impermissible due to the right to privacy between a banking institution and its client.
> As to the constitutionally guaranteed rights of a person, the court in *Prosecutor-General v Lameck and Others* [2010 (1) NR 156 (HC)] echoed the same sentiments when stating at 172B – C:
>
> > *'It cannot be emphasised enough that the powers under ss 24 and 25 are so invasive of people's constitutionally guaranteed rights and, potentially, their dignity and ultimately freedom, that this court must exact the highest standard of propriety from those whose interventions might affect those rights.'*
>
> ....
> It is trite that 'the Constitution is based on the rule of law, affirms the democratic values of dignity and freedom, and guarantees the right to privacy, a fair trial and just administrative action'. Because of punitive measures provided for in respect of certain provisions in the Act, it requires that the procedural powers of the ACC must be interpreted in such a way that it least impinges on the rights and values of a person. **The purpose of incorporating the right to privacy in the Constitution is that no one should be subjected to unreasonable invasions of a person's liberty, privacy, property or effects. Any invasion of these rights must be authorised by law in such manner that it least intrudes [on] those rights enshrined in the Constitution.** As far as it concerns the issue at hand, the issuing of any search and seizure warrant or summons by the ACC, as provided for in the Act, are instances where such encroachment is authorised by law.
> …
> …The commission, by the issuing of summonses prior to the initiation of an investigation contemplated in s 18(3), had clearly acted outside its mandate by adopting procedure not prescribed by law.
> …
> …**The correct procedures were available, but not followed. This rendered the summonses invalid and renders evidence obtained consequential thereto unlawful.** The Constitution guarantees an accused a fair trial — which includes pre-trial procedures — whereby the accused's dignity and interests must at all times be respected and protected by the courts. To allow evidence that was unlawfully obtained (emanating from invalid summonses) would result in a gross violation of the accused persons' fundamental rights to privacy and a fair trial, guaranteed under the Constitution.
> …
> The commission's conduct in this regard must be discouraged in the strongest of terms as the courts cannot allow persons or institutions to be subjected to an abuse of power on its part. Although the ACC fulfils an important function in society with its main purpose to fight the seemingly unending

[8] *JS v LC* 2016 (4) NR 939 (SC), paragraph 55, emphasis added.

[9] *S v Lameck* 2019 (2) NR 368 (HC).

> scourge of corruption in this country, the commission must be reminded that it is also subject to the Constitution and the law, moreover, that it must give effect to the provisions of the Act, its creator, which brought it into existence.
> …
> In the result, summonses issued by the ACC on 11 June 2009 are invalid and evidence emanating from the impugned summonses is ruled inadmissible.[10]

(2) Similarly, a 2018 High Court case **set aside six search warrants for failure to follow the proper procedure:**

> **Whereas the right to privacy is guaranteed under art 13 of the Constitution it deserves a very high level of protection and demands a strict interpretation of the search and seizure provisions in the Act**. Those provisions may, for obvious reasons, result in a serious encroachment on the rights of those persons subjected to them. Hence, the courts will construe search and seizure warrants strictly and furthermore carefully scrutinise anything done in pursuance thereof. What this means is that the courts are obliged to employ a strict interpretation of the provisions relating to search and seizure warrants.[11]

Other observations made about the right to privacy, in Namibian cases decided on other grounds, may be helpful pointers to future jurisprudence in this area.

(1) In a 2006 case, the High Court quoted with approval this statement from a South African Constitutional Court judgment:

> It should also be noted that there is a **close link between human dignity and privacy** in our constitutional order. The right to privacy… recognises that **human beings have a right to a sphere of intimacy and autonomy that should be protected from invasion**. This right serves to foster human dignity.

The Namibian Court observed that those remarks "also hold true under our Constitution".[12]

(2) In a case concerning the right to a fair trial, the Supreme Court took note of the similarity in various constitutional formulations on permissible limitations of constitutional rights, taking into account their judicial interpretation. The Court observed that the criteria for limitation of the right to privacy set out in Art 13(1) operate in much the same manner as the authority in Art 21(2) for limitations to the fundamental freedoms enumerated in art 21(1) – **suggesting that case law on limitations to Art 21 freedoms may be applicable to limitations on the right to privacy under Art 13(1).**[13]

This indicates, looking to leading cases such *Kauesa v Minister of Home Affairs & Others* 1996 (4) SA 965 (NmS), that a court would require a lawful limitation on the right to privacy to be **reasonable, necessary, rationally connected to a legitimate State objective and proportional to that objective**. The *Kauesa* case also stated that, in assessing limitations to rights and freedoms, a court must be "guided by the values and principles that are essential to a free and democratic society which respects the inherent dignity of the human person, equality, non-discrimination, social justice and other such values" (page 977), and that courts "should be strict in interpreting limitations to rights so that individuals are not unnecessarily deprived of the enjoyment of their rights" (page 980).

---

[10] Footnotes and bracketed evidence numbers have been omitted. The excerpt is taken from paragraphs 13-33 of the judgement.

[11] *S v Lameck* 2018 (3) NR 902 (HC), paragraph 9. See also *S v Lameck* 2017 (3) NR 647 (SC) This case was an appeal against the lower court's ruling on an application for recusal, but it touches tangentially on the right to privacy, as the underlying dispute concerned the validity of certain warrants. See, in addition, *Samco Import & Export CC v Magistrate of Eenhana* 2009 (1) NR 290 (HC), at paragraphs 25-29 on the need to construe the law on search warrants strictly. *New Force Logistics CC v Anti-Corruption Commission* 2018 (2) NR 375 (HC) includes similar sentiments; see, for instance, paragraphs 59-61.

[12] *Afshani v Vaatz* 2006 (1) NR 35 (HC), paragraph 29.

[13] *Attorney-General of Namibia v Minister of Justice* 2013 (3) NR 806 (SC), paragraphs 29-30.

There is no Namibian case as yet that provides a detailed focus on the contours of the right to privacy or the appropriate approach to analysing interference with that right.

2.3 Namibia's international obligations

International treaties that are binding on Namibia are part of Namibian law by virtue of Article 144 of the Namibian Constitution. **The key international treaty on the right to privacy is the *International Covenant on Civil and Political Rights (ICCPR).*** Article 17 of the ICCPR states that no one "shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence nor to unlawful attacks on his honour and reputation", and provides that everyone has "the right to the protection of the law against such interference or attacks".

The Human Rights Committee has expressed concern about the invasion of privacy by data retention schemes in its concluding observations on reports from several countries.

For instance, the Committee set out its interpretation of Article 19 in respect of bulk phone metadata surveillance carried out by the United States. It indicated that Article 17 requires that "measures should be taken to **ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity**, regardless of the nationality or location of the individuals whose communications are under direct surveillance". It also emphasised that infringement on the right to privacy, family, home or correspondence must:

- be authorized by laws that are publicly accessible;
- be tailored to specific legitimate aims;
- be articulated in terms are sufficiently precise and detailed about the circumstances in which any interference with the right is permissible;
- specify the procedures for authorization, the categories of persons who may be placed under surveillance, the limit on the duration of surveillance and procedures for the use and storage of data collected; and
- provide for effective safeguards against abuse.

Most importantly for the present discussion, the Committee has also **urged States Parties to refrain "from imposing mandatory retention of data by third parties", and to ensure that "affected persons have access to effective remedies in cases of abuse"**.[14]

In considering the country report of the United Kingdom, **the Human Rights Committee made similar observations about UK legislation that provides wide powers for the retention of communications data, without limiting access to such data to cases involving "the most serious crimes"**.[15]

As another example, the Human Rights Committee urged Italy to review its regime regulating retention of communications data to ensure that it conforms with the obligations under Article 17 of the ICCPR, "including the principles of legality, proportionality and necessity", **emphasising the need for judicial authorization in all cases, effective remedies in cases of abuse, and *ex post facto* notification to individuals who have been placed under surveillance**.[16]

In a report on ***The Right to Privacy in the Digital Age***,[17] the UN High Commissioner for Human Rights also discussed the test for interference with the rights guaranteed by Article 17 of the ICCPR, emphasising the principles of legality, necessity and proportionality:

---

[14] "Concluding observations on the fourth periodic report of the United States of America", Human Rights Committee, CCPR/C/USA/CO/4, 14 April 2014, para 22, www.refworld.org/docid/5374afcd4.html.

[15] "Concluding observations on the fourth periodic report of the United Kingdom of Great Britain and Northern Ireland", Human Rights Committee, CCPR/C/GBR/CO/7, 17 August 2015, para 24, www.refworld.org/docid/5645a59c4.html.

[16] "Concluding Observations on the Sixth Periodic Report of Italy", Human Rights Committee, CCPR/C/ITA/CO/6, 1 May 2017, para 37, www.refworld.org/docid/591e9a6b4.html.

[17] "The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights", A/HRC/27/37, 30 June 2014, www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a-hrc-27-37_en.doc

(1) With respect to **legality**, the limitation to privacy rights must be provided for by a law that is sufficiently accessible, clear and precise to enable an individual to know who is authorized to conduct data surveillance and under what circumstances.
(2) In terms of **necessity** the law must serve a legitimate aim as well as having some chance of achieving the stated goal.
(3) Regarding **proportionality**, the law must impose the least intrusive option available. The degree of limitation to the right must not render the essence of the right meaningless, and it must be consistent with other human rights such as the prohibition of discrimination (para 23).

In light of these principles, the Report makes the following observation on "the increasing reliance of Governments on private sector actors to retain data 'just in case' it is needed for government purposes" (para 26):

> **Mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate** (para 26).[18]

The Report acknowledges that governments justify digital communications surveillance programmes on the grounds of national security, including risks from terrorism, stating that, while this may indeed be a legitimate aim, the degree of interference must still be assessed "against the necessity of the measure to achieve that aim and the actual benefit it yields towards such a purpose" (para 25).

> **In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate** (para 25).

A 2015 **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression** considered encryption and anonymity in communications in light of the rights to privacy and freedom of opinion and expression found in the ICCPR as well as other universal and regional human rights instruments. This Report notes that encryption and anonymity "provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks" (para 16). The Special Rapporteur notes that restrictions on "encryption and anonymity, as enablers of the right to freedom of expression, must meet the well-known three-part test: any limitation on expression must be provided for by law; may only be imposed for legitimate grounds … and must conform to the strict tests of necessity and proportionality" (para 31):

> 32. **First, for a restriction on encryption or anonymity to be "provided for by law", it must be precise, public and transparent, and avoid providing State authorities with unbounded discretion to apply the limitation. Proposals to impose restrictions on encryption or anonymity should be subject to public comment and only be adopted, if at all, according to regular legislative process.** Strong procedural and judicial safeguards should also be applied to guarantee the due process rights of any individual whose use of encryption or anonymity is subject to restriction. In particular, a court, tribunal or other independent adjudicatory body must supervise the application of the restriction.
>
> 33. **Second, limitations may only be justified to protect specified interests: rights or reputations of others; national security; public order; public health or morals**. Even where a State prohibits by law "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, as provided by Article 20 of the Covenant, any restrictions on expression must be consistent with Article 19(3). No other grounds may justify restrictions on the freedom of expression. Moreover, because legitimate objectives are often cited as a pretext for illegitimate purposes, the restrictions themselves must be applied narrowly.
>
> 34. **Third, the State must show that any restriction on encryption or anonymity is "necessary" to achieve the legitimate objective**. The European Court of Human Rights has concluded appropriately that the word "necessary" in article 10 of the European Convention for the Protection of Human Rights and Fundamental

[18] On this point, the report references the Addendum to General Comment No. 27, Human Rights Committee, CCPR/C/21/Rev.1/Add.9, 1 November 1999, paras 11-16, https://undocs.org/CCPR/C/21/Rev.1/Add.9.

> Freedoms means that the restriction must be something more than "useful," "reasonable" or "desirable". Once the legitimate objective has been achieved, the restriction may no longer be applied. Given the fundamental rights at issue, limitations should be subject to independent and impartial judicial authority, in particular to preserve the due process rights of individuals.
>
> 35. **Necessity also implies an assessment of the proportionality of the measures limiting the use of and access to security online.** A proportionality assessment should ensure that the restriction is "the least intrusive instrument amongst those which might achieve the desired result". The limitation must target a specific objective and not unduly intrude upon other rights of targeted persons, and the interference with third parties' rights must be limited and justified in the light of the interest supported by the intrusion. The restriction must also be "proportionate to the interest to be protected". A high risk of damage to a critical, legitimate State interest may justify limited intrusions on the freedom of expression. **Conversely, where a restriction has a broad impact on individuals who pose no threat to a legitimate government interest, the State's burden to justify the restriction will be very high.** Moreover, a proportionality analysis must take into account the strong possibility that encroachments on encryption and anonymity will be exploited by the same criminal and terrorist networks that the limitations aim to deter. In any case, "a detailed and evidence-based public justification" is critical to enable transparent public debate over restrictions that implicate and possibly undermine freedom of expression (paras 32-35, emphasis added; footnotes and references omitted).

The Report asserts that **anonymity plays an important role** in safeguarding and advancing privacy, free expression, political accountability, public participation and debate (para 47) and is particularly important for activists and protestors (para 53). It notes that laws requiring SIM card registration directly undermine anonymity and "may provide Governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest" (para 51).

The Special Rapporteur expressed specific concern about the impact of data retention requirements in this regard:

> 55. Broad mandatory data retention policies limit an individual's ability to remain anonymous. A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint. A State's ability to collect and retain personal records expands its capacity to conduct surveillance and increases the potential for theft and disclosure of individual information (para 55).

He also **recommended against requiring identification for all SIM card users and online users**:

> … States should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users…Court-ordered decryption, subject to domestic and international law, may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals (para 60).

3. European Union (EU)

Data Retention Directive

In 2006, the EU adopted the **Data Retention Directive** (Directive 2006/24/EC) which mandated "the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks".[19] The objective of the Directive was to serve as a tool "in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime". In fact, the Directive followed in the wake of the 2005 terrorist attacks in London.

The Directive required EU Member States to ensure that communications providers retained the data specified in the Directive for a time period set by national law and falling between 6 months and 2 years (Art 6).

[19] Available for download at https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32006L0024.

The data covered by the Directive fell into six categories, covering data necessary to identify: (1) the source of a communication; (2) the destination of a communication; (3) the date, time and duration of a communication; (4) the type of the communication; (5) the user's communication equipment; and (6) the location of any mobile communication equipment. It explicitly did *not* authorise retention of the *content* of the communication (Art 5).

The Directive left the rules and procedures for accessing this data to national law, subject to the general principles that the data could be made available only to competent national authorities and that the procedures and conditions for access must be cognizant of necessity and proportionality requirements (Art 4). The Directive also specified that providers of communications services which retained such data must be required to apply certain "data security principles": (1) The retained data must be of the same quality as data on the network, and subject to the same degree of security and protection. (2) It must be protected against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure. (3) There must be safeguards to ensure that the data can be accessed only by specially authorised personnel. (4) The retained data must be destroyed at the end of the specified period (Art 7).

Digital Rights Ireland (2014)

The Data Retention Directive was challenged on the grounds that it impermissibly interfered with a number of rights protected by the Charter of Fundamental Rights of the European Union, including the right to privacy, the right to the protection of personal data, the right to freedom of expression and the right to good administration. The ensuing ***Digital Rights Ireland*** case was decided by the Grand Chamber of the Court of Justice of the European Union.[20]

The Court found that the breadth of the data covered by the retention requirements constituted a severe encroachment into the right of privacy, even though content was excluded:

> Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.
>
> Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (paras 26-27).

It found that the intrusiveness of such data retention requirements might discourage the use of certain means of communication, thereby impinging on the exercise of the freedom of expression (para 28).

Furthermore, because the requirements involved the processing of personal data, they invoked the data protection principles provided by the Charter (para 29).

The key question was whether the intrusion into these rights was justifiable. Article 52(1) of the Charter provides that any limitation on the exercise of protected rights and freedoms must be (a) provided for by law; (b) respect the essence of the rights in question; and (c) interfere with protected rights only to the extent necessary to meet objectives of general interest or to protect the rights and freedoms of others, subject to the principle of proportionality.

The Court was satisfied that the Directive did not affect the essence of any of the cited rights, and that the objectives of enhancing public security, and combating international terrorism and organised crime, were valid ones. The problem was the proportionality of the infringements (paras 38-ff).

The Court found that the Directive should have provided "**clear and precise rules** governing the scope and application of the measure in question and imposing **minimum safeguards** so that the persons whose data

[20] *Case C-293/12 - Digital Rights Ireland LTD v Minister for Communications, Marine and Natural Resources, and Others* and *C-594/12 - Kartner Landesregierung and Others*, 8 April 2014, full text in English at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&from=EN

have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data" (para 54).

Furthermore, **the interference was not limited to what is strictly necessary**, because it required the retention of traffic data in respect of fixed telephones, mobile telephones, Internet access, Internet e-mail and Internet telephones – thus covering essentially all means of electronic communication and **entailing an interference with the fundamental rights of practically the entire European population, without requiring any evidence suggesting that their conduct might have any link whatsoever with serious crime** (paras 56, 58). In addition, there was no requirement of a specific relationship between the data retained and a threat to public security, nor any limitations to particular time periods, geographical areas or circles of persons likely to be involved in criminal activities or likely to be able to contribute to the prevention, detection or prosecution of crimes (paras 56-59).

An additional problem was the **lack of any objective criteria for determining when access to the data by competent national authorities would be allowed**, nor any provisions on the **conditions of access**. The Court suggested that the Directive should have made access to the retained data dependent on a prior review carried out by a court or an independent administrative body, with a view to limiting access to the data and its use "to what is strictly necessary for the purpose of attaining the objective pursued" (paras 60-62).

Also, the **period for the retention of the data was not based on any objective criteria** (paras 63-64).

The Court concluded that the Directive thus "entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary" (para 65). It also concluded that the Directive failed to provide sufficient safeguards "to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data" (para 66-ff). The Directive therefore failed to satisfy the requirements of proportionality and was ruled invalid (para 71).[21]

Tele2 Sverige AB/Watson and the EU E-Privacy Directive (2016)

In the aftermath of the *Digital Rights Ireland* case, EU Member States were expected to make their national legislation compliant with the Court's judgment and other EU Directives. This gave rise to more questions about what was permissible under EU law.

Two cases involving Sweden and the UK were joined (***Tele2 Sverige AB* and *Watson***[22]) and considered in December 2016 in a preliminary ruling by the Grand Chamber on the question of how another EU Directive, the **E-Privacy Directive** (Directive 2002/58/EC), applies to national telecommunications data retention schemes.

The E-Privacy Directive contains provisions protecting various rights:

- EU Member States must enact legislation protecting "the **confidentiality** of communications and the related traffic data by means of a public communications network and publicly available electronic communications services", and provides that Member States must accordingly ensure that information and access to stored information takes place only with the **consent** of the affected person (Art 5).
- **Traffic data** (any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof) may be **stored only as long as it is required for communication transmission, billing or (with the user's consent) marketing**, and must be **erased** after that (Art 6).

[21] See also Court of Justice of the European Union. "PRESS RELEASE No 54/14", 8 April 2014, https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf;
Theresa Papademetriou, "European Union: ECJ Invalidates Data Retention Directive", Library of Congress Law, June 2014, www.loc.gov/law/help/eu-data-retention-directive/eu.php.

[22] Joined Cases C-203/15: *Tele2 Sverige AB v Post-och telestyrelsen* and C-698/15: *Watson & others v Secretary of State for the Home Department (United Kingdom of Great Britain and Northern Ireland),* 21 December 2016, full text of the judgment available in English at https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=17504.

- **Location data** (data indicating the geographic position of the terminal equipment of the user (may be processed only when made **anonymous**, or with the **consent** of users or subscribers, and **only to the extent and for the time necessary for the provision of a value-added service** (Art 9(1)).
- **EU Member States may adopt legislative measures that restrict these rights "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system"**. For these ends, the legislative measures may provide for the retention of data for a limited period justified by the purpose (Art 15(1)).

The Court found that the E-Privacy Directive has the following impact on national legislation on data retention:

(1) **It precludes national legislation that, for the purpose of fighting crime, provides for the general and indiscriminate retention of *all* traffic and location data of *all* subscribers and registered users relating to *all* means of electronic communication.** This approach is disproportionate to the objective, because it provides for the retention of data of persons with no link whatsoever to serious criminal activity or public security (judgment, paras 94-112).

(2) **It requires that national legislation governing access to retained data by competent national authorities to the retained data must ensure that such access does not exceed the limits of what is strictly necessary.** It must also contain "**clear and precise rules** indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data".

Access must generally be limited to the data of individuals suspected of planning, committing or having committed a serious crime, or of being implicated in some way with a serious crime – although access to the data of other persons might also be granted where there is objective evidence in a specific case that such data make an effective contribution to combating activities such as terrorism that could threaten national security, defence or public security interests. **This means that access must generally be subject to prior review by a court or an independent administrative body, except in cases of "validly established urgency".**

The law must also provide for notice of the access to the data to be given to the affected persons, as soon as this is no longer likely to jeopardise the investigations being undertaken by national authorities.

Moreover, there must be provision for review by an independent authority of the data retention scheme's compliance with the data protection principles that apply to the processing of any personal data. This includes measures to protect the retained data against misuse and unlawful access, provision for the data to be retained within the European Union and destruction of the data at the end of the authorised data retention period (paras 113-125).

In short, the Court's decision did *not* indicate that all data retention requirements would be unlawful. It left the door open for Member States to introduce legislation on ***targeted*** **data retention for the purpose of preventing serious crime** (in contrast to "general and indiscriminate" data retention) – provided that such measures are limited to what is strictly necessary in terms of the categories of data retained, the persons affected and the time period covered.[23]

In many EU countries, litigation and amendments to laws in force continue in the wake of these decisions of the European Court, as countries consider how to apply the principles articulated in the judgments.[24]

[23] Orla Lynskey, "Tele2 Sverige AB and Watson et al: Continuity and Radical Change", *European Law Blog*, 12 January 2017, https://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/.

[24] See, for instance "National Data Retention Laws Since the CJEU's *Tele-2/Watson* Judgment: A Concerning State of Play for the Right to Privacy in Europe", Privacy International, September 2017, pages 15-ff, https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf.

Breyer v Germany (2020)

In this recent case, the European Court of Human Rights considered provisions of Germany's Telecommunications Act that required telecommunications service providers to collect and store certain personal data regarding their customers, after Germany's Federal Constitutional Court had held that they were compatible with German's Basic Law (Grundgesetz).

The law in question obligated telecommunications service providers to store certain information in respect of all users, whether the service provider in question allocated telephone numbers directly or provided connections for telephone numbers allocated by other parties:

1. The telephone numbers and other identifiers of the respective allocation;
2. The name and address of the allocation holder;
3. The date of birth in the case of natural persons;
4. In the case of fixed lines, additionally the address for the line;
5. In cases in which a mobile-communication end device is made available together with the mobile-communication allocation, also the device number of the said device, as well as;
6. The effective date of the contract (majority judgment, para 27).

This legal provision had been amended in 2016 to oblige service providers to verify the personal data against presentation of an identity card, a passport or other official identity document (para 28). This obligation applied to users of pre-paid mobile phone SIM cards as well as customers who entered into phone service contracts (para 59).

The law required that the entities storing the information must make it available to the Federal Network Agency by automated means, so that this Agency could make it available on request to any of various State authorities to the extent that knowledge of the data was necessary for them to carry out their legal functions. The list of authorities included, amongst others:

- the courts and criminal prosecution authorities;
- law-enforcement authorities "for purposes of averting danger";
- customs investigation offices, for various customs-related purposes;
- intelligence agencies;
- emergency service centres;
- the Federal Financial Supervisory Authority.

The main question before the Court was whether the law impermissibly infringed the right to private and family life in the Charter of Fundamental Rights of the European Union (paras 46, 60-63). The parties agreed that the law infringed these rights, so the issue was whether the infringement was justifiable – with the key point being whether the interference was proportionate and struck a fair balance between the competing public and private interests (paras 88-91).

The Court placed significant weight on the fact that the law required storage of only a limited data set relating to identification of the user, without calling for the storage of any individual communication events or data that could track users' movements; it relied on this distinction to distinguish this case from the previous ones decided by the Court of Justice of the European Union (discussed above), even though the law required the collection and storage of this limited data in respect of *all* users instead of only persons under some kind of suspicion (paras 92-93).

In terms of access to the data, the Court found that even though the list appears broad, all of the authorities cited were concerned with law enforcement or the protection of national security (para 98). It found further

As one example, in April 2021, the Belgian Constitutional Court annulled a Belgian law requiring telecommunications providers to retain electronic communications data in bulk, on the grounds that it did not comply with the requirements set out in the decisions of the Court of Justice of the European Union. See, for instance, "Belgian Constitutional Court Annuls Data Retention Framework for Electronic Communications Data", *Privacy and Information Security Law Blog*, Hunton Andrew Kurth (law firm), 23 April 2021, www.huntonprivacyblog.com/2021/04/23/belgian-constitutional-court-annuls-data-retention-framework-for-electronic-communications-data/.

protection against "excessive or abusive information requests" by the fact that "the requesting authority requires an additional legal basis to retrieve the data", and the provision that limits information retrieval to necessary data. Another safeguard was the law's requirement that any authority that retrieves information must erase any data they do not need without undue delay (para 100). The Court also noted that each retrieval must be recorded to allow for supervision by independent data protection authorities, which also have power to consider complaints from anyone who believes that his or her rights have been infringed through the collection, processing or use of his or her personal data by public bodies (paras 105, 107).

The Court thus concluded that the challenged law did *not* constitute an impermissible interference with the right to private and family life.

The dissenting opinion by one judge took the view that there was an unjustified infringement of the right to private and family life, emphasising the following points:

- **Access to the personal data in question was not confined to issues of terrorism or other serious crimes or national security risks**, but extended to other authorities such as customs investigation services, emergency services, the financial supervisory authority and several intelligence agencies (dissenting opinion, para 3).
- **Even though the law did not mandate the storage of any sensitive personal information, it covered data that enables a person to be *linked* with a phone number or a phone number and thus with communications made through that number, which could reveal sensitive personal information** (para 5).
- Because **the law affected *all* telecommunications users**, the case was comparable to the *Digital Rights Ireland* case and the *Tele2 Sverige/ Watson* cases which invalidated similar laws (para 7).
- The **majority judgment failed to consider the importance of anonymity** in promoting the free flow of ideas and information (para 8).
- The failure to fully consider the impact of the law meant that **the majority opinion underestimated the level of interference with the right to private and family life** (para 9) – which in turn affected the assessment of proportionality.
- Although the law required a legal basis for accessing the identifying data, it **did not set a threshold limiting data collection to the investigation of serious crimes or specific serious threats to national security** (para 15).
- The **search function authorised by the law does not limit the data retrieved to specific telephone numbers or names**, but may pull up personal data concerning a large number of persons who have not even an indirect or remote link to criminal or regulatory offences (paras 16-17).
- There are **insufficient safeguards against misuse and abuse of personal data** in the regulatory scheme. Retrievals of personal data did not require an order by a judicial or otherwise independent authority, and those requesting access via the Federal Network Agency did not have to motivate their requests with reasons. Information requests could take place without the knowledge of the telecommunications service provider or the relevant subscriber, and there is no legal duty to notify a mobile telephone subscriber at any stage that his or her personal details have been retrieved – which prevent any review of the information retrieval, especially where there is no further investigation or surveillance of the individual in question. The supervision by the data protection authority cited by the majority was not adequate given the huge number of data sets at issue (paras 10-26).

The dissenting judge thus concluded that the law violated the Charter's protection for private and family life (para 27).[25]

[25] See also Judith Vermeulen, "Bulk retention of private-sector subscriber data for governmental purposes does not violate the Convention: Breyer v. Germany", *Strasbourg Observers*, 5 March 2020, https://strasbourgobservers.com/2020/03/05/bulk-retention-of-private-sector-subscriber-data-for-governmental-purposes-does-not-violate-the-convention-breyer-v-germany/.

4. India

In India, biometric-backed identification numbers are issued by the Unique Identification Authority of India (UIDAI) under the Aadhaar Act. ("Aadhaar" is a Hindi word that means "foundation" or "base".) Each person legally resident in India can enrol in the Aadhaar system by submitting personal information along with certain biometrics (currently fingerprints and an iris scan). The person in question is then assigned a unique twelve-digit identity number that is intended to serve as the primary form of identification. The identification data is stored in a centralised data base. Aadhaar cards are issued to those who have registered, but the crux of the scheme is the unique identification number which can be authenticated against the individual's biometrics. The law governing the scheme gives State authorities a duty to secure all of the identification information that they hold, and prescribes rules for data-sharing. It is not legally mandatory to enrol in the Aadhaar scheme, but so many state services require secure identification that it is compulsory in a practical sense.

The constitutionality of the overarching Aadhaar scheme was challenged on numerous grounds in a case decided by the Supreme Court in 2018. The issue most relevant to this discussion is the assertion that the entire identification scheme violated the right to privacy, which is not directly articulated in the Indian Constitution but has been established and developed through jurisprudence. The Court described privacy as being a right that "ensures that a human being can lead a life of dignity by securing the inner recesses of the human personality from unwanted intrusions" and is furthermore "intrinsic to freedom, liberty and dignity" (majority opinion, para 81).

It was argued that the scheme constituted an invasion into the personal right to privacy because it could "lead to a surveillance state where each individual can be kept under surveillance by creating his/her life profile and movement as well on his/her use of Aadhaar" (majority opinion, para 3). The opposing views on the overall scheme were summarised by the Court as follows:

> Those in favour see Aadhaar project as ushering the nation into a regime of good governance, advancing socio-economic rights, economic prosperity etc. and in the process they claim that it may make the nation a world leader… Those opposing Aadhaar are apprehensive that it may excessively intrude into the privacy of citizenry and has the tendency to create a totalitarian state, which would impinge upon the democratic and constitutional values (para 4).

In Indian jurisprudence, privacy has three aspects: (i) intrusion with an individual's physical body; (ii) informational privacy; and (iii) privacy of personal choices. To test whether or not there has been an unwarranted interference with the right to privacy, the Court must apply a three-part test of proportionality: (a) the interference with the right must be **sanctioned by law**; (b) the proposed interference must be **necessary in a democratic society for a legitimate aim**; and (c) the extent of such interference must be **proportionate** to the need for such interference (paras 82-83, 117).

Applying this test, the Court found that **the overall identification scheme passed the test of constitutionality**, by imposing a minimal interference with privacy which was necessary for the legitimate State purpose of enrolling unprivileged and marginalised members of the society, in order to empower them by giving them access to welfare schemes that would enhance their dignity (para 309). The Court held that the Aadhaar Act "has struck a fair balance between the right of privacy of the individual with right to life of the same individual as a beneficiary" (para 313).

Once the Court had established the constitutionality of the underlying Aadhaar scheme, it considered some specific aspects of that scheme separately.

One of these was a **2017 directive requiring all mobile service subscribers (pre-paid or post-paid, and new or existing) to link their mobile numbers to their Aadhaar number** (para 439). In addition to objecting to the fact that this requirement was contained in a circular rather than a law, the Court also noted the existence of less intrusive alternatives: "For the misuse of such SIM cards by a handful of persons, the entire population cannot be subjected to intrusion into their private lives." The Court thus found the requirement to be an unconstitutional interference with the right to privacy (para 442).

A separate judgement by Justice Chandrachud disagreed with the majority on the overarching constitutionality of the Aadhaar scheme but agreed with the majority holding on the unconstitutionality of linking mobile phone usage with Aadhaar identity. This separate opinion elaborated on the issue of proportionality, after noting that the State does "have a legitimate concern over the existence of SIM cards obtained against identities which are not genuine" (opinion of Chandrachud J, para 283).

> But the real issue is whether the linking of Aadhaar cards is the least intrusive method of obviating the problems associated with subscriber verification. The state cannot be oblivious to the need to protect privacy and of the dangers inherent in the utilization of the Aadhaar platform by telecom service providers. **In the absence of adequate safeguards, the biometric data of mobile subscribers can be seriously compromised and exploited for commercial gain**. While asserting the need for proper verification, **the state cannot disregard the countervailing requirements of preserving the integrity of biometric data and the privacy of mobile phone subscribers**. Nor can we accept the argument that cell phone data is so universal that one can become blasé about the dangers inherent in the revealing of biometric information….
>
> …The mere existence of a legitimate state aim will not justify the means which are adopted. Ends do not justify means, at least as a matter of constitutional principle. For the means to be valid, they must be carefully tailored to achieve a legitimate state aim and should not be either disproportionate or excessive in their encroachment on individual liberties…
>
> **Mobile technology has become a ubiquitous feature of our age. Mobile phones are not just instruments to facilitate a telephone conversation. They are a storehouse of data reflecting upon personal preferences, lifestyles and individual choices. They bear upon family life, the workplace and personal intimacies. The conflation of biometric data with SIM cards is replete with grave dangers to personal autonomy. A constitution based on liberal values cannot countenance an encroachment of this nature.** The decision to link Aadhaar numbers to SIM cards and to enforce a regime of e-KYC [Know Your Customer] authentication clearly does not pass constitutional muster and must stand invalidated (excerpted from paras 283-285).

In January 2021, the Supreme Court received a group of petitions requesting re-examination of the majority holding in the 2018 case – but, by a vote of 4-1, declined to review the 2018 decision.[26]

5. South Africa

In South Africa, the Constitutional Court recently invalidated the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA) on the grounds that it constituted an impermissible interference with the constitutional right to privacy.[27]

This Act covered various forms of surveillance and interception of communications – including data retention by telecommunications providers and access to that data by State officials, which was covered by Chapter 7 of RICA (sections 39-41). The Constitutional Court judgment did not focus on this aspect of the law, but many

---

[26] See "SC rejects pleas seeking review of 2018 Aadhaar verdict", *Financial Express*, 21 January 2021, www.financialexpress.com/aadhaar-card/sc-rejects-pleas-seeking-review-of-2018-aadhaar-verdict-2/2175184/; Utkarsh Anand, "4-1 verdict: Supreme Court dismisses pleas seeking Aadhaar ruling review", *India News*, 21 January 2021, www.hindustantimes.com/india-news/41-verdict-supreme-court-dismisses-pleas-seeking-aadhaar-ruling-review-101611189869910.html; Krishnadas Rajagopal, "Five-judge Supreme Court Bench to review verdict upholding Aadhaar on January 11", *The Hindu*, 10 January 2021, www.thehindu.com/news/national/five-judge-supreme-court-bench-to-review-verdict-upholding-aadhaar-on-january-11/article33541810.ece
There was no substantive consideration of the issues in the Court's 2020 decision. According to press reports, the Court stated: "We have perused the review petitions as well as the grounds in support thereof. In our opinion, no case for review of judgment and order dated September 26, 2018 is made out. We hasten to add that in the law or subsequent decision/judgement of a coordinate or larger bench by itself cannot be regarded as a ground for review. The review petitions are accordingly dismissed." Justice Chandrachud again dissented. See, for example, "Supreme Court rejects Aadhaar review plea in 4:1 verdict", *Times of India*, 21 January 2021, https://timesofindia.indiatimes.com/india/supreme-court-rejects-aadhaar-review-plea-in-41-verdict/articleshow/80375919.cms.

[27] *Amabhungane Centre for Investigative Journalism NPC & Another v Minister of Justice and Correctional Services & Others; Minister of Police v Amabhungane Centre for Investigative Journalism NPC & Others* 2021 (3) SA 246 (CC), https://collections.concourt.org.za/bitstream/handle/20.500.12144/36631/%5bJudgment%5d%20CCT%20278%20of%2019%20and%20279%20of%2019%20AmaBhungane%20Centre%20for%20Investigative%20Journalism%20v%20Minister%20of%20Justice%20and%20Others.pdf?sequence=42&isAllowed=y.
The Act, which has been amended several times, was sourced through the subscription service Juta's Statutes of South Africa.

of its concerns about surveillance in general would be applicable to this form of data retention and access as well.[28]

As a background to the Constitutional Court's consideration of the Act's general impact on the right to privacy, the Court noted that the country's **apartheid history** was characterised by "the wanton invasion of the privacy of people by the state through searches and seizures, the interception of their communications and generally by spying on them in all manner of forms" (majority Constitutional Court judgement, para 26) – a point that is equally relevant to Namibia. The Court also noted at the outset that invasion of an individual's privacy also infringes that individual's right to **dignity**, which is of fundamental importance (para 28). However, it also took note of the argument that the law serves the **important purpose of facilitating investigation and combating of serious crime, protecting national security and maintaining public order** – thereby ensuring the safety of the population (para 29).

Against this backdrop, the Court considered specific components of the legal challenge to RICA. Only those which could have relevance to Namibia's regulatory scheme on telecommunications data are discussed here.

Notification

The Court was disturbed by the lack of provision for notification to the subject of the surveillance, even after the fact. When authority is given for a traditional search, this eventually comes to the notice of the person who is searched. But when surveillance is authorised, the person whose communications are intercepted may never know. **This complete secrecy makes surveillance under the Act susceptible to abuse.** The lawfulness of the authority for the surveillance can never be challenged if the surveillance remains unknown – which could lead to a culture of impunity on the part of law enforcement officials. The upshot is that "an individual whose privacy has been violated in the most intrusive, egregious and unconstitutional manner never becomes aware of this and is thus denied an opportunity to seek legal redress for the violation of her or his right to privacy" (paras 38-44). The Court thus held that **post-surveillance notification should be the default position, unless the State can present justifiable reasons why an exception should be made in a specific case** (paras 45-48).

Although this part of the constitutional challenge applied to surveillance, it would be equally relevant to law enforcement access to retained communications data about an individual; in order to prevent abuses of the process, it can be argued there should be a requirement that the individual receives notification of the access once this would not jeopardise the object of the investigation.

Safeguards for ex parte process

In respect of authority for surveillance, an issue of concern is that the application is necessarily *ex parte* – since the surveillance would be pointless if the subject were aware of it in advance. This means that the application is granted "on the basis of information provided only by the state agency requesting the direction". **The judge must make a decision on the basis of one-sided information** and, unless there are obvious shortcomings, inaccuracies or falsehoods, the decision-maker is not in a position "meaningfully to interrogate the information" (para 96). The applicants asserted that this undermines the principle that both sides must be heard, and so violates the right to fair hearing; **other forms of *ex parte* proceedings are usually granted only on an interim basis, but orders that allow interception of communications are final**. Therefore the applicants suggested that some form of adversarial process should be applied to ensure "that the interests of the subject of surveillance are properly protected and ventilated". They suggested that a "public advocate" could play this role.

The Constitutional Court held that the absence of sufficient safeguards to address the fact that authority to intercept communications is sought and obtained *ex parte* was a factor that rendered the law

[28] This portion of the Act was challenged in the High Court on the grounds that it lacked adequate safeguards regarding the archiving of data and subsequent access to it. More specifically, the applicants challenged the requirement that the specified data must be retained by electronic communications service providers for 2 to 5 years, and the procedures for managing this data in question (examining, copying, sharing, sorting through, using, destroying or storing it). The High Court dismissed the challenge regarding the period of retention on the grounds that this was within the province of Parliament to decide, but upheld the challenge regarding insufficient safeguards for the management of the data in question (as described in the majority Constitutional Court judgement, para 18).

unconstitutional. However, it declined to recommend a specific mechanism to remedy this problem, ruling that the "choice of safeguards to address the inadequacies resulting from the *ex parte* nature of the process is something best left to Parliament" (para 95-100).

Again, although this issue was discussed in the context of the *interception* of communications, it also has relevance for *ex parte* applications for *access to retained communications data* about an individual.

Management of information

The applicants also challenged the law's lack of safeguards for **how information from intercepted communications is handled, stored and eventually destroyed**. The Court was concerned that the legal scheme provided no clarity or detail on:

> what must be stored; how and where it must be stored; the security of such storage; precautions around access to the stored data (who may have access and who may not); the purposes for accessing the data; and how and at what point the data may or must be destroyed. Thus there is a real risk that the private information of individuals may land in wrong hands or, even if in the "right" hands, may be used for purposes other than those envisaged in RICA. All this exacerbates the risk of unnecessary intrusions into the privacy of individuals (para 107).

The Court concluded that the law was rendered unconstitutional to the extent of its failure to adequately prescribe procedures "to ensure that data obtained pursuant to the interception of communications is managed lawfully and not used or interfered with unlawfully, including prescribing procedures to be followed for examining, copying, sharing, sorting through, using, storing or destroying the data" (para 108).

This would seem to apply also to retained communications data – perhaps even more forcibly since this data is stored by telecommunications service providers rather than by State officials. In fact, one amicus in the South African case urged the Court to rule that this concern applied with equal force to data retained by private telecommunications service providers; the Court declined to do so on the grounds that this issue had not been fully ventilated due to the manner in which it was raised, but it did observe that **"in our age of mass data surveillance, private actors arguably pose a comparable threat to privacy as does the state**" (para 111).

Overall, the Court found RICA to be unconstitutional to the extent that it fell short in respect of these and other safeguards. It suspended the declaration of unconstitutionality for 36 months to afford Parliament an opportunity to cure the defects that were noted, and read certain safeguards into the law as an interim measure.[29]

6. Possible constitutional problems with the Namibian regime

An examination of the relevant international standards and comparative jurisprudence points to some worrying problems with Namibia's regulatory scheme.

(1) Overbreadth leading to lack of proportionality

One characteristic of the scheme of immediate note is that **telecommunications service providers are required to collect and store data about *every user who meets the definition of "customer"* – thus retaining a massive amount of data of which only a tiny proportion is likely to ever be requested by the police or intelligence services.** This would likely mean that the approach taken could not satisfy the principle that justifiable interference with a constitutional right must be as minimal as possible, and only what is reasonably necessary to serve the objective.

As has been seen in respect of other jurisdictions, it is more likely that a *targeted* data retention scheme will pass constitutional muster - with data being retained and stored in the first place *only in respect of persons who are reasonably suspected of having some connection to serious crime.*

[29] There was one dissenting opinion which focused on an issue peculiar to the South African law which is not relevant to the discussion here.

This is a **data preservation approach** rather than a data retention approach:

> Data preservation is an alternative to data retention that can help law enforcement while minimizing the impact on human rights. Under a data preservation regime, a law enforcement officer can demand that an Internet company begin storing – "preserving" – data relevant to a specified investigation or proceeding. Typically, the company is required to continue preserving this data for a period of time, such as 90 days.[30]

Indeed, this is the approach that is taken by the latest version of Namibia's Cybercrime Bill (in the draft circulated by the Ministry of Information, Communications and Technology for comment in June 2021):

> **Preservation**
>
> **20.** (1) If a member of the Namibian police is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation might be lost, modified or destroyed, that member may issue a written notice instructing a person in control of that computer data to ensure that the data described in the notice must be preserved for the period specified in the notice which period may not be longer than seven days.
>
> (2) A notice referred to in subsection (1) may be extended by a judge or magistrate for a period that does not exceed three months at a time.

The types of data that must be collected and retained may also be found to go beyond what is strictly necessary for the law's purposes. As been noted elsewhere, the listed data would be sufficient to provide a detailed profile of communications activity that can reveal many aspects of a person's private life, including their relationships, interests and movements. This list should be re-considered in light of the principle of proportionality.

(2) Lack of suitability to serve the objective

Another question of concern is **what purpose the data retention requirements can actually serve given the exclusion of (a) pre-paid telecommunications services and (b) services accessed via foreign telecommunications service providers.** Anyone with a communication to hide would surely simply utilise one of the excluded channels – meaning that the interference with the privacy of other customers would be likely to be for naught.

Yet there might be problems entailed with broadening the scheme.[31] For instance, in September 2014, the **Romanian Constitutional Court invalidated an Emergency Ordinance that required registration of all pre-paid SIM cards and the users of free public Wifi hotspots**, on top of more general requirements about the retention of data of users of telecommunications services.[32] As with general telecommunications data retention, the motivation for the new legal provisions was "the need to adopt measures to facilitate criminal investigation activities or those for knowing, preventing and counteracting risks or threats to national security". The law was enacted after police tragically failed to save a teenage girl who had been abducted but managed to call the 112 emergency number three times before she was murdered.

The Court noted that the basic data retention regime contemplated the completion of a standard form when entering into a contract for telecommunications services, in advance of the provision of those services. But in the case of pre-paid services and access to public Wifi networks, the sale is often via an intermediary dealer – which raises serious questions about who would bear the duty to guarantee the confidentiality and security of

---

[30] See, for example, "Introduction To Data Retention Mandates", Center for Democracy & Technology, September 2012, page 6, https://cdt.org/wp-content/uploads/pdfs/CDT_Data_Retention-Five_Pager.pdf.

[31] For an overview of the issue of requiring identification of SIM care users, see "The Mandatory Registration of Prepaid SIM Card Users: A White Paper", GMSA, November 2013, www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf.

GSMA, which is commonly referred to only by its acronym, is the *Global System for Mobile Communications Association*, with "GSM" originally denoting *Groupe Spécial Mobile.* It represents the interests of mobile operators worldwide.

[32] The challenge to the law was mounted by the Romanian Ombudsman, at the urging of several human rights groups. The case is "Decizia Curții Constituționale nr. 461/2014 – lege prepay și înregistrare utilizatori WiFi, DECIZIA Nr.461 din 16 septembrie 2014", https://privacy.apti.ro/decizie-curtea-constitutionala-prepay-461-2014/, available only in Romanian, with machine translation into English.

the data and prevent unauthorised use. In the case of public Wifi networks, the Court noted that such services are often accessed through private entities such as commercial and leisure areas, cafes, restaurants, hotels and airports, or via public institutions such as educational facilities, public libraries and medical clinics (para 41). The Court continued (as machine-translated):

> The imposition on these persons of the obligation to retain and store personal data requires, in a correlative manner, the express regulation of appropriate, firm and unequivocal measures, such as to ensure the confidence of citizens that the personal data they have provide are registered and kept confidential. In this respect, the law is limited to establishing measures for data retention and storage, without amending or supplementing the legal provisions on the guarantees that the state must provide in the exercise of the fundamental rights of citizens. However, the regulatory framework in such a sensitive area must be carried out in a clear, predictable and non-confusing manner, so as to remove, as far as possible, the possibility of arbitrariness or abuse of those called upon to apply the legal provisions (para 41).[33]

The Court invalidated the provisions at issue on the basis that they lacked the precision and predictability necessary for proportional interference with individual rights, and failed to ensure the confidentiality of personal data - thus infringing the very essence of fundamental rights regarding privacy, family and private life and the secrecy of correspondence, as well as freedom of expression (paras 44, 46).[34]

(3) No *ex post facto* notice to affected individuals and no other safeguards for *ex parte* proceedings

It is a point in favour of the Namibian law that access to retained data would ordinarily require authorisation by a court. However, the concerns raised by the South African Constitutional court in respect of *ex parte* proceedings are relevant here.

The affected persons may never know that their data has been accessed – in contrast to traditional searches and seizures which generally become known by their nature. This creates a situation where the validity of the access may never be challenged. While the person who is being monitored could normally not be informed of the situation at the time without defeating the purpose of the investigation, provision could be made for **notice to the affected person after the investigation was finalised** (regardless of its outcome).

In addition, an *ex parte* request for access to stored data has a final rather than an interim outcome, yet the procedure incorporates no adversarial component. Some have proposed that a public advocate could be used to play such a role; perhaps the Office of the Ombudsman could serve such a function in Namibia.

(4) Inappropriate decision-making process in urgent situations

As detailed above in section 2, **the regulations make provision for the police (but not the intelligence services) to access customer information from a telecommunications service provider *without court authorisation* in urgent situations.** Even if this exception to court authorisation were found to be warranted, the procedure **places the key decision-making burden on the authorised persons appointed by telecommunications service providers instead of on trained police officers**. It seems inappropriate to give this responsibility to a private individual rather than to the police officer concerned.

(5) No attention to data security principles

Although Namibia does not yet a data protection law in place, guidance on basic data protection principles can be drawn from the **African Union Convention on Cyber Security and Personal Data Protection, 2014**

---

[33] For more information on the Romanian case and data retention laws, see Bogdan Manolea, "Romania: Mandatory prepaid SIM registration ruled unconstitutional", European Digital Rights (EDRi), 24 September 2014, https://edri.org/our-work/romania-mandatory-prepaid-sim-registration-ruled-unconstitutional/; Valentina Pavel, "Romania: Mandatory SIM registration declared unconstitutional, again", European Digital Rights (EDRi), 26 February 2020, https://edri.org/our-work/romania-mandatory-sim-registration-declared-unconstitutional-again/; Rosi Bakó, "Romania", Global Information Society Watch (GISWatch) [2014], https://giswatch.org/en/country-report/communications-surveillance/romania; Valentina Pavel "Icing on the cake: Romanian cybersecurity law unconstitutional", European Digital Rights (EDRi), 28 January 2015, https://edri.org/our-work/romanian-cybersecurity-law-declared-unconstitutional/.

[34] A subsequent attempt to introduce a similar law was also declared unconstitutional. See Valentina Pavel "Romania: Mandatory SIM registration declared unconstitutional, again", European Digital Rights (EDRi), 26 February 2020, https://edri.org/our-work/romania-mandatory-sim-registration-declared-unconstitutional-again/. which reports that this case invalidated the law in question on procedural grounds without conducting a substantive analysis.

which has been signed and ratified by Namibia but has not yet received sufficient support to come into force.[35] Whether or not the approach to telecommunications data is narrowed, **the scheme needs to comply with basic data protection principles** – including measures pertaining to the **security** of the data and protections for **confidentiality** and the **prevention of unauthorised access**, as well as provision for the **erasure or destruction of data** after the requisite time period for its retention has expired.

Conclusion

Based on the survey of comparative law outlined here, it seems likely that Namibia's telecommunications data retention scheme might be found to be an unconstitutional infringement of the right to privacy overall, given the intrusion into the privacy of large segments of the population in a manner that has a questionable ability to serve the intended objectives. At the very least, it seems to be unconstitutionally faulty in some key aspects relating to the breadth of its coverage and the kinds of data required to be collected, the lack of procedural safeguards and the lack of attention to data protection principles. It does not seem to be appropriately proportional to its aims.

[35] The AU status list can be accessed here.