Institut suisse de droit comparé
Schweizerisches Institut für Rechtsvergleichung
Istituto svizzero di diritto comparato
Swiss Institute of Comparative Law

E-Avis ISDC 2025

SURVEILLANCE OF TELECOMMUNICATION PROVIDERS

Austria, Denmark, France, Germany, Russian Federation, Spain, Sweden, United Kingdom, United States of America

Current to: 30.09.2025

Cet avis de droit est publié avec l'approbation explicite de la personne qui a mandaté l'ISDC.
Dieses Gutachten wird mit ausdrücklicher Zustimmung der Person veröffentlicht, die das SIR beauftragt hat.
Il presente parere giuridico è pubblicato con il consenso esplicito della persona che ha dato all'ISDC il mandato di redigerlo.
This legal opinion is published with the express permission of the person who instructed the SICL.

Krista Nadakavukaren Schefer *et al*.

E-Avis ISDC
Série de publications électroniques d'avis de droit de l'ISDC / Elektronische Publikationsreihe von Gutachten des SIR / Serie di pubblicazioni elettroniche di pareri dell'Istituto svizzero di diritto comparato / Series of Electronic Publications of Legal Opinions of the SICL

Recommended citation: Krista Nadakavukaren Schefer *et al*., Surveillance of telecommunication providers, Austria, Denmark, France, Germany, Russian Federation, Spain, Sweden, United Kingdom, United States of America, *E-Avis ISDC 2025*, (www.isdc.ch)

Basé sur l'avis No 25-059-E

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The study of nine legal jurisdictions within and outside of the European Union demonstrated that while there are several fundamental differences between EU Member States' regulations of telecommunications providers and the regulatory regimes of other states, in other aspects the differences are minor. The difference in treatment increases when looking outside of the EU.

Categorization and differential treatment of telecommunication service providers

None of the jurisdictions considered distinguish telecommunications providers into the specific categories of providers of telecommunications services (*Anbieter von Fernmeldediensten*, *FDA*) and providers of derived communications services (*Anbieter von abgeleiteten Kommunikationsdiensten, AAKD*) that Switzerland does. As EU Member States, most of the jurisdictions examined instead adopt the EU's terminology and categorization of "number-based" and "number-independent" telecommunication service providers for the application of the general telecommunications law, although the specifics of what services are in each category may vary.

France is different than Austria and Germany, categorizing operators and providers separately. Spain distinguishes telecommunications service providers in accordance with the EU categorization but regulates providers of information society services and electronic commerce services separately from telecommunications services. Sweden currently has separate treatment for number-based and number-independent providers but is considering a broadening of its data retention obligations to include all providers. Denmark is an exception to the number-based/number-independent dichotomy, with its regulatory framework applying to all telecommunication service providers.

Of the non-EU Member States, there are more variations in how providers are categorized. The Russian framework distinguishes among telecommunications service providers and networks, the latter not being subject to as many obligations as the former. The UK legal framework applies to all telecommunications service providers and is conceived to cover a broad range of providers. The United States distinguishes providers that offer sending or receiving services from those that store or process data for the public.

Surveillance obligations

Surveillance obligations in the studied jurisdictions are mainly those of enabling police or security authorities to gain access to data. This includes ensuring that the infrastructure permits interception and may require that the systems can interface with each other. It also requires that service providers cooperate with the authorities. The extent of this obligation may depend on the type of data and the seriousness of the suspected crime.

In the United Kingdom, telecommunication service providers must also inform the authorities of any planned changes to their services or functionalities, including for changes that might affect the ability to assist law enforcement investigations. The United States has a detailed and differential approach to surveillance obligations. While the main relevant pieces of legislation impose numerous obligations, including that of designing systems that can intercept communications, excluded providers - including "information services" such as Signal – do not have as wide a range of obligations.

No jurisdictions require active surveillance by telecommunication service providers and all require normal requests for data to be accompanied by a warrant or judicial approval.

Data retention

The EU Member States' rules on data retention vary substantially, depending on the type of data and the particular jurisdiction. This is permitted by the Court of Justice of the European Union's row of cases following the *Digital Rights Ireland* case. While Digital Rights Ireland strongly pushed toward privacy protection, the cases following it (*Tele2Sverige & Privacy International*, the *La Quadrature du Net I* and *II* cases, and *SpaceNet*) provided for Member States to allow for retention of traffic data for addressing national security threats and the retention of a more limited set of data in particular geographic areas. EU Member States took advantage of the possibility to require more data retention, but to different degrees.

In Denmark, the rules set forth general retention duties of "traffic data" for one year in particular for purposes of national security; in France, operators must retain most data for one year, although there are longer periods for certain types of institutions that hold data and shorter periods for other types of data. Spain's law implementing the 2006 EU Data Retention Directive imposes a general retention period of one year (although exceptions exist). Other Member States' rules emphasize privacy obligations, requiring that data is deleted within a certain period unless a request is presented for it to be retained. In most jurisdictions, data retention obligations apply to the communication's source and destination and method of transmission.

The Russian data retention requirements appear to be more expansive than those of the other regimes studied. The different types of providers have varying obligations and the obligations will also depend on the type of data, which includes the information contained in the communication. In the United Kingdom, there are no general data retention obligations. It is only if the authorities ask for data to be retained that the providers will be under an obligation to comply. The United States also has no requirement that data (including boundary data) be retained. Moreover, privacy concerns are increasing.

Removal of Encryption

The rules on removal of encryption vary among the jurisdictions studied. In Austria, Germany, Russia, Spain, and the United States there are no general requirements that telecommunications providers decrypt messages for the government. While in Spain there is an exception to that rule if the provider encrypted the message itself first, in Russia, providers must give the government the keys to allow it to decrypt the messages. In the UK, providers need to decrypt messages upon the government's request only to the extent of reasonableness and not if the encryption is end-to-end. In France, telecommunication service providers are among the possible persons that may have to decrypt messages required by police investigations, but the provider cannot be made to decrypt if it does not have the key or if it would contravene basic rights or professional obligations.

I. QUESTIONS

This report was prepared at the request of the Federal Department of Justice and Police (EJPD). The information contained within is based on the written resources available to the Institute's legal division. In setting out the legal framework of each jurisdiction, the reports may not reflect the practice of authorities in implementing the legal rules.

1. Are there different categories of telecommunication providers that are similar to those of the telecommunication service providers (*Anbieter von Fernmeldedienste*n, FDA) and providers of derived communications services (*Anbieter von abgeleiteten Kommunikationsdiensten*, AAKD) in Swiss law?

2. What surveillance and information obligations do telecommunication service providers have?

3. How does the law regulate data retention?

4. How does the law regulate the retention of boundary date (*Randdaten*)?

5. How long must providers retain data?

6. Rules regarding the removal of encryption. What types of encryption must be removed? Who must un-encrypt communications? What content must be sent to authorities in readable form? Are there exceptions to the encryption removal requirements?

II. ANALYSIS

A. AUSTRIA

Das **Telekommunikationsgesetz 2021** (TKG 2021)[1] regelt die Pflichten von Anbietern in Österreich. Darüber hinaus enthält auch die Überwachungsverordnung (ÜVO)[2] relevante Normen.

1. Kategorien an Telekommunikationsdienstleistern (Anbieter von Fernmeldediensten (FDA), Anbieter von abgeleiteten Kommunikationsdiensten)

Das TKG 2021 unterscheidet bei interpersonellen Kommunikationsdiensten[3] zwischen sogenannten **nummerngebundenen** (§ 4 Z 7 TKG 2021)[4] und **nummernunabhängigen** interpersonellen Kommunikationsdiensten (4 Z 8 TKG 2021)[5].

---

1 Verfügbar unter https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20011678 (23.05.2025).

2 Verfügbar unter https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001655 (23.05.2025).

3 Diese sind in § 4 Z 6 TKG 2021 legaldefiniert als «ein gewöhnlich gegen Entgelt erbrachter Dienst, der einen direkten interpersonellen und interaktiven Informationsaustausch über Kommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die Kommunikation veranlassen oder daran beteiligt sind; dazu zählen keine Dienste, die eine interpersonelle und interaktive Kommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen».

4 Ein nummerngebundener Dienst ist «ein interpersoneller Kommunikationsdienst, der entweder eine Verbindung zu öffentlich zugeteilten Nummerierungsressourcen, nämlich Nummern nationaler oder internationaler Nummerierungspläne, herstellt oder die Kommunikation mit Nummern nationaler oder internationaler Nummerierungspläne ermöglicht», § 4 Z 7 TKG 2021.

5 Ein nummernunabhängiger Dienst hingegen ist «ein interpersoneller Kommunikationsdienst, der weder eine Verbindung zu öffentlich zugeteilten Nummerierungsressourcen, nämlich Nummern nationaler oder internationaler Nummerierungspläne, herstellt noch die Kommunikation mit Nummern nationaler oder internationaler Nummerierungspläne ermöglicht, § 4 Z 8 TKG 2021.

2. Überwachungs- und Informationspflichten

Die **gesetzlichen Grundlagen für eine Überwachung der Telekommunikation** finden sich in § 135 Strafprozessordnung 1975 (StPO)[6], § 11 Staatsschutz- und Nachrichtendienstgesetz (SNG)[7], § 99 Finanzstrafgesetz (FinStrG)[8] und § 22 Militärbefugnisgesetz (MBG)[9].[10]

Die Anbieter, das heisst die Betreiber von öffentlichen Kommunikationsdiensten,[11] sind verpflichtet, alle **Einrichtungen bereitzustellen, die zur Überwachung von Nachrichten und zur Auskunft über Daten erforderlich sind**.[12] Von den hierfür entstehenden Personal- und Sachaufwendungen werden den Anbietern 80 % ersetzt.[13] Darüber hinaus müssen Anbieter an der Überwachung von Nachrichten und der Auskunft über Daten mitwirken.[14]

Die Gesetze unterscheiden zwischen verschiedenen Sorten von Daten, nämlich zwischen **Stammdaten**, **Verkehrsdaten**, **Zugangsdaten**, **Inhaltsdaten** und **Standortdaten**.[15] Strafverfolgungsbehörden dürfen bei Vorliegen der entsprechenden Voraussetzungen auf Ersuchen von Kriminalpolizei, Staatsanwaltschaft oder Gericht Auskunft über Stammdaten verlangen.[16] Für Auskunft über Zugangsdaten[17] sowie für eine Anlassdatenspeicherung[18] ist eine Anordnung durch die Staatsanwaltschaft erforderlich.[19] Für Auskünfte über Daten einer Nachrichtenübermittlung[20], für die Lokalisierung einer technischen Einrichtung[21] sowie für die Überwachung von Nachrichten ist eine Anordnung durch die Staatsanwaltschaft auf Grundlage einer gerichtlichen Bewilligung erforderlich.[22]

---

6 Verfügbar unter https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326 (23.05.2025).

7 Verfügbar unter https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009486 (23.05.2025).

8 Verfügbar unter https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10003898 (23.05.2025).

9 Verfügbar unter https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20000864 (23.05.2025).

10 Vgl. § 161 Abs 3 S. 2, § 162 Abs 1 S. 1, Abs 2 S. 1 TKG 2021.

11 Legaldefiniert in § 160 Abs 3 Z 1 TKG 2021.

12 § 162 Abs 1 Z 1 TKG 2021.

13 § 162 Abs 1 Z 2 TKG 2021.

14 § 162 Abs 2 S. 1 TKG 2021.

15 § 160 Abs 3 Z 5-9 TKG 2021. Zu den Definitionen der verschiedenen Daten siehe unter den Punkten 3.1. bis 3.4. in diesem Gutachten.

16 § 135 Abs 1a Var 1 i.V.m. § 137 Abs 1 S. 2 StPO.

17 § 135 Abs 1a StPO.

18 § 135 Abs 2b StPO.

19 § 137 Abs 1 S. 3 StPO.

20 § 135 Abs 2 StPO.

21 § 135 Abs 2a StPO.

22 § 137 Abs 1 S. 4 StPO.

3. Speicherung von Daten

Bei der Speicherung von Daten durch die Anbieter ist **nach der Art der Daten zu unterscheiden**. Grundsätzlich dürfen Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten nur ermittelt oder verarbeitet werden, wenn dies einer Besorgung eines Kommunikationsdienstes dient.[23]

3.1. Stammdaten

Das Gesetz definiert **Stammdaten** als «Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Nutzerverzeichnissen erforderlich sind»[24]. Sie dürfen abgesehen von wenigen gesetzlich geregelten Ausnahmen nur für die folgenden Zwecke verarbeitet werden:

- Abschluss, Durchführung, Änderung oder Beendigung des Vertrags,
- Verrechnung der Entgelte,
- Erstellung von Nutzerverzeichnissen[25],
- Erteilung von Auskünften an Betreiber von Notdiensten[26].[27]

Die genannten **gesetzlich geregelten Ausnahmen** gestatten die Übermittlung von Stammdaten, soweit dies für die betreffende Erbringung des Kommunikationsdienstes erforderlich ist sowie die Verarbeitung zum Zwecke der Vermarktung oder der Bereitstellung von Diensten mit Zusatznutzen, sofern eine jederzeit widerrufbare Einwilligung der betroffenen Person vorliegt.[28] Zudem müssen Anbieter Auskunft über Stammdaten an Gerichte, Staatsanwaltschaften und die Kriminalpolizei geben, sofern ein schriftliches Verlangen hierfür vorliegt und dies zur Aufklärung und Verfolgung eines Verdachts einer Straftat geschieht.[29] Ebenfalls bei Vorlage eines schriftlichen und begründeten Verlangens müssen Anbieter ausserdem Verwaltungsbehörden Auskunft über Stammdaten geben, wenn der Verdacht besteht, über ein öffentliches Telekommunikationsnetz eine Verwaltungsübertretung begangen zu haben. Hierfür dürfen die Daten jedoch nicht verarbeitet werden und es dürfen keine Auskünfte über die Bonität gegeben werden.[30]

3.2. Verkehrsdaten

Verkehrsdaten sind diejenigen «Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden».[31] Verkehrsdaten dürfen grundsätzlich weder gespeichert noch übermittelt werden und müssen nach Beendigung der jeweiligen Verbindung unverzüglich gelöscht oder anonymisiert werden.[32]

Sollte dies zur Abwicklung von Prepaid- oder Endkundenleistungen erforderlich sein, so muss der Betreiber eines öffentlichen Kommunikationsnetzes oder -dienstes Verkehrsdaten speichern, bis die

---

23 § 165 Abs. 1 TKG 2021.

24 § 160 Abs 3 Z 5 TKG 2021; der Begriff der Stammdaten umfasst den Namen, den akademischen Grad, die Anschrift, die Nutzernummer oder sonstige Kontaktinformation, Informationen über Art und Inhalt des Vertragsverhältnisses, die Bonität sowie das Geburtsdatum, siehe lit. a) bis g) der Norm.

25 Im Sinne des § 126 TKG 2021.

26 Im Sinne des § 124 TKG 2021.

27 § 166 Abs 1 Z 1-4 TKG 2021.

28 § 165 Abs 2 TKG 2021.

29 § 181 Abs 9 TKG 2021.

30 § 181 Abs 8 TKG 2021.

31 § 161 Z 6 TKG 2021.

32 § 167 Abs 1 Satz 1 TKG 2021.

Leistung bezahlt ist.[33] Unter bestimmten Voraussetzungen **müssen die Daten jedoch gespeichert werden**, nämlich wenn:

- Fristgerecht Einspruch erhoben wurde,
- Die Rechnung nicht beglichen wurde,
- Ein Verfahren über die Höhe der Entgelte eingeleitet wurde oder
- eine Anordnung gemäss § 135 Absatz 2b StPO[34] erlassen wurde oder aufgrund einer Anordnung der Staatsanwaltschaft.[35]

Zu **Auskunftszwecken** ist es in bestimmten Zwecken zudem zulässig, Verkehrsdaten zu verarbeiten.[36]

---

33 § 167 Abs 2 Satz 1 TKG 2021.

34 § 135 Abs 2b in Verbindung mit Abs 2 Z 2-4 und § 76 Abs 2 StPO:
«§ 135 Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Anlassdatenspeicherung und Überwachung von Nachrichten
(2) Auskunft über Daten einer Nachrichtenübermittlung ist zulässig,
[…] 2. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt, oder
3. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können.
4. wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann.
(2b) Anlassdatenspeicherung ist zulässig, wenn dies aufgrund eines Anfangsverdachts (§ 1 Abs. 3) zur Sicherung einer Anordnung nach Abs. 2 Z 2 bis 4 oder einer Anordnung nach § 76a Abs. 2 erforderlich erscheint.»
«§76 Amts- und Rechtshilfe
(2) Ersuchen von kriminalpolizeilichen Behörden, Staatsanwaltschaften und Gerichten, die sich auf Straftaten einer bestimmten Person beziehen, dürfen mit dem Hinweis auf bestehende gesetzliche Verpflichtungen zur Verschwiegenheit oder darauf, dass es sich um automationsunterstützt verarbeitete personenbezogene Daten handelt, nur dann abgelehnt werden, wenn entweder diese Verpflichtungen ausdrücklich auch gegenüber Strafgerichten auferlegt sind oder wenn der Beantwortung überwiegende öffentliche Interessen entgegenstehen, die im Einzelnen anzuführen und zu begründen sind.»

35 § 167 Abs 2 Satz 3 Z 1-4 TKG 2021.

36 § 167 Abs 5 Z 1-5 TKG 2021:
«§ 167 Verkehrsdaten
(5) Eine Verarbeitung von Verkehrsdaten zu Auskunftszwecken ist zulässig zur Auskunft über
1. Daten einer Nachrichtenübermittlung gemäß § 134 Z 2 StPO;
2. Zugangsdaten an Gerichte und Staatsanwaltschaften nach Maßgabe des § 135 Abs. 1a zweiter Fall StPO;
3. Verkehrsdaten und Stammdaten, wenn hierfür die Verarbeitung von Verkehrsdaten erforderlich ist, sowie zur Auskunft über Standortdaten an nach dem SPG zuständige Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a und 3b SPG, § 11 Abs. 1 Z 5 SNG sowie § 22 Abs. 2b MBG. Ist eine aktuelle Standortfeststellung nicht möglich, darf die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang der Endeinrichtung verarbeitet werden;
4. Zugangsdaten, wenn diese längstens drei Monate vor der Anfrage gespeichert wurden, an nach dem SPG zuständige Sicherheitsbehörden nach Maßgabe des § 53 Abs. 3a Z 3 SPG, des § 11 Abs. 1 Z 5 SNG, des § 99 Abs. 3a FinStrG sowie des § 22 Abs. 2b MBG;
5. Verkehrsdaten, Zugangsdaten und Standortdaten nach Maßgabe des § 11 Abs. 1 Z 7 SNG sowie des § 22 Abs. 2b MBG.»

3.3. Inhaltsdaten

Inhaltsdaten im Sinne des TKG 2021 sind die Inhalte übertragener Nachrichten.[37] Grundsätzlich dürfen Inhaltsdaten **nicht gespeichert** werden, sofern die Speicherung nicht einen wesentlichen Bestandteil des Kommunikationsdienstes darstellt.[38] Dementsprechend muss der Anbieter technische oder organisatorische Vorkehrungen treffen, um sicherzustellen, dass Inhaltsdaten nicht oder nur in dem aus technischen Gründen erforderlichen Mindestmass gespeichert werden.[39]

3.4. Standortdaten

Der Begriff der **Standortdaten** umfasst «Daten, die in einem Kommunikationsnetz oder von einem Kommunikationsdienst verarbeitet werden und die den geografischen Standort der Endeinrichtung eines Benutzers eines öffentlichen Kommunikationsdienstes angeben, im Fall von festen Endeinrichtungen sind Standortdaten die Adresse der Einrichtung».[40]

Standortdaten, die nicht zugleich Verkehrsdaten sind, dürfen grundsätzlich **nur verarbeitet werden, wenn sie entweder anonymisiert sind oder der Benutzer oder Nutzer eine jederzeit wiederrufbare Einwilligung gegeben hat**.[41] Auch bei Vorliegen einer solchen Einwilligung muss es dem Benutzer oder Nutzer möglich sein, die Verarbeitung einfach und kostenlos vorübergehend zu verbieten.[42] Eine solche Verarbeitung der Standortdaten muss auf das für den betreffenden Dienst erforderliche Mass und die erforderlichen Personen beschränkt werden.[43] Grundsätzlich ist die Ermittlung und Verwendung von Standortdaten zu Auskunftszwecken allerdings unzulässig, wenn die Daten nicht im Zusammenhang mit einem Kommunikationsvorgang stehen. Eine Ausnahme hiervon gilt lediglich für Notrufe sowie für die unter Punkt 2. aufgezählten gesetzlich geregelten Fälle.[44]

4. Speicherung von Randdaten

Der Begriff der Randdaten wird im TKG 2021 nicht verwendet. **Verkehrsdaten** hingegen bezeichnen solche Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden.[45] Zur Speicherung von Verkehrsdaten siehe unter Punkt 3.2. in diesem Gutachten.

Die **Vorratsdatenspeicherung** wurde 2014 vom Verfassungsgerichtshof für **verfassungswidrig und gegen die Europäische Menschenrechtskonvention verstossend** erklärt.[46] Die entsprechenden Vorschriften sind in der heute gültigen Fassung der Strafprozessordnung nicht mehr enthalten. Das

---

37 § 160 Z 8 TKG 2021.

38 § 168 Abs 1 S. 1 TKG 2021.

39 § 168 Abs 2 S. 1 TKG 2021.

40 § 160 Z 9 TKG 2021.

41 § 169 Abs 1 Z 1, 2 TKG 2021.

42 § 169 Abs 2 TKG 2021.

43 § 169 Abs 3 S. 1 TKG 2021.

44 § 169 Abs 3 S. 2 in Verbindung mit § 161 Abs 3 TKG 2021.

45 § 161 Z 6 TKG 2021.

46 VGH, Entscheidung vom 27.06.2014 – G 47/2012-49, G 59/2012-38, G 62/2012-46, G 70/2012-40, G 71/2012-36, verfügbar unter https://www.vfgh.gv.at/downloads/VfGH_G_47-2012_ua_VDS_schriftliche_Entscheidung.pdf (23.05.2025).

Gesetz[47] führte aus, welche Daten jeweils von Anbietern von Internet-Zugangsdiensten[48], von Anbietern öffentlicher Telefondienste einschliesslich Internet-Telefondiensten[49] sowie von Anbietern von E-Mail-Diensten[50] gespeichert werden mussten. Dabei unterschied das Gesetz zwischen Anbietern von Internet-Zugangsdiensten, Anbietern öffentlicher Telefondienste einschliesslich Internet-Telefondiensten sowie Anbietern von E-Mail-Diensten. Ausgenommen waren solche Unternehmen, die nicht der Verpflichtung zur Entrichtung eines Finanzierungsbeitrags unterlagen.[51] Der Inhalt der Kommunikation und insbesondere Daten über im Internet aufgerufene Adressen durften in diesem Rahmen jedoch nicht gespeichert werden.[52] Für eine Auskunft über Vorratsdaten war, bei Vorliegen

---

47 § 102a TKG 2003 a.F. ist verfügbar unter https://www.ris.bka.gv.at/eli/bgbl/i/2003/70/P102a/NOR40128485 (27.06.2025).

48 § 102a Abs 2 TKG 2003 a.F.:
«§ 102a Vorratsdaten
(2) Anbietern von Internet-Zugangsdiensten obliegt die Speicherung folgender Daten:
1. Name, Anschrift und Teilnehmerkennung des Teilnehmers, dem eine öffentliche IP-Adresse zu einem bestimmten Zeitpunkt unter Angabe der zugrunde liegenden Zeitzone zugewiesen war;
2. Datum und Uhrzeit der Zuteilung und des Entzugs einer öffentlichen IP-Adresse bei einem Internet-Zugangsdienst unter Angabe der zugrundeliegenden Zeitzone;
3. die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss;
4. die eindeutige Kennung des Anschlusses, über den der Internet-Zugang erfolgt ist.»

49 § 102a Abs 3 TKG 2003 a.F.:
«§ 102a Vorratsdaten
(3) Anbietern öffentlicher Telefondienste einschließlich Internet-Telefondiensten obliegt die Speicherung folgender Daten:
1. Teilnehmernummer oder andere Kennung des anrufenden und des angerufenen Anschlusses;
2. bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Teilnehmernummer, an die der Anruf geleitet wird;
3. Name und Anschrift des anrufenden und des angerufenen Teilnehmers;
4. Datum, Uhrzeit des Beginns und Dauer eines Kommunikationsvorganges unter Angabe der zugrundeliegenden Zeitzone;
5. die Art des in Anspruch genommenen Dienstes (Anrufe, Zusatzdienste und Mitteilungs- und Multimediadienste).
6. Bei Mobilfunknetzen zudem
a) der internationalen Mobilteilnehmerkennung (IMSI) des anrufenden und des angerufenen Anschlusses;
b) der internationalen Mobilfunkgerätekennung (IMEI) des anrufenden und des angerufenen Anschlusses;
c) Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Standortkennung (Cell-ID), an dem der Dienst aktiviert wurde, wenn es sich um vorbezahlte anonyme Dienste handelt;
d) der Standortkennung (Cell-ID) bei Beginn einer Verbindung.»

50 § 102a Abs 4 TKG 2003 a.F.:
«§ 102a Vorratsdaten
(4) Anbietern von E-Mail-Diensten obliegt die Speicherung folgender Daten:
1. die einem Teilnehmer zugewiesene Teilnehmerkennung;
2. Name und Anschrift des Teilnehmers, dem eine E-Mail-Adresse zu einem bestimmten Zeitpunkt zugewiesen war;
3. bei Versenden einer E-Mail die E-Mail-Adresse und die öffentliche IP-Adresse des Absenders sowie die E-Mail-Adresse jedes Empfängers der E-Mail;
4. beim Empfang einer E-Mail und deren Zustellung in ein elektronisches Postfach die E-Mail-Adresse des Absenders und des Empfängers der Nachricht sowie die öffentliche IP-Adresse der letztübermittelnden Kommunikationsnetzeinrichtung;
5. bei An- und Abmeldung beim E-Mail-Dienst Datum, Uhrzeit, Teilnehmerkennung und öffentliche IP-Adresse des Teilnehmers unter Angabe der zugrunde liegenden Zeitzone.»

51 § 102a Abs 6 TKG 2003 a.F.

52 § 102a Abs 7 TKG 2003 a.F.

der entsprechenden Voraussetzungen, eine Anordnung durch die Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung erforderlich.[53]

5. Dauer der Datenspeicherung

5.1. Stammdaten

Stammdaten müssen spätestens nach **Vertragsende** gelöscht werden, sofern diese nicht noch benötigt werden, um den Vertrag abzuwickeln, Beschwerden zu bearbeiten oder sonstige gesetzliche Pflichten zu erfüllen.[54]

5.2. Verkehrsdaten

Müssen **Verkehrsdaten** ausnahmsweise gespeichert werden, um die Entgelte von Prepaid- und Endkundenleistungen zu verrechnen, so müssen die Verkehrsdaten gelöscht oder anonymisiert werden, **sobald die Leistungen bezahlt und nicht innerhalb einer Frist von drei Monaten schriftlich beeinsprucht wurden**.[55]

5.3. Inhaltsdaten

Grundsätzlich dürfen **Inhaltsdaten** nicht gespeichert werden. Sollte dies jedoch aus **technischen Gründen** für eine kurze Dauer erforderlich sein, so müssen die Inhaltsdaten **nach Wegfall dieser Gründe** unverzüglich gelöscht werden.[56]

Handelt es sich bei der Speicherung um einen **wesentlichen Bestandteil des Kommunikations-dienstes**, müssen die Daten **unmittelbar nach Erbringung des Dienstes** gelöscht werden.[57]

5.4. Vorratsdatenspeicherung

Die **Vorratsdatenspeicherung** ist derzeit **nicht möglich**.[58]

6. Vorgaben zur Entfernung von Verschlüsselungen

Im Juli 2025 hat der österreichische Bundesrat eine Gesetzesänderung[59] angenommen, durch welche in Zukunft die **Überwachung von verschlüsselter und unverschlüsselter Kommunikation über Messengerdienste ab Oktober 2025 möglich** sein wird.

---

53 § 102b Abs 1 TKG 2003 a.F.

54 § 166 Abs 3 S. 1, 2 TKG 2021.

55 § 167 Abs 2 Satz 2 TKG 2021.

56 § 168 Abs 1 S. 2 in Verbindung mit S. 1 TKG 2021.

57 § 168 Abs 2 S. 2 TKG 2021.

58 Als sie 2014 eingeführt wurde, sah sie jedoch eine Speicherung der Daten für höchstens sechs Monate vor, vgl. § 102a Abs 1 S. 1 Telekommunikationsgesetz 2003 (TKG 2003), abgedruckt in BGBl. 2011 Teil I, 27. Bundesgesetz, verfügbar unter https://www.vfgh.gv.at/downloads/VfGH_G_47-2012_ua_VDS_schriftliche_Entscheidung.pdf (23.05.2025).

59 136 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVIII. GP, Regierungsvorlage, verfügbar unter https://www.parlament.gv.at/dokument/XXVIII/I/136/fname_1693648.pdf (30.09.2025), Art 1 Z 10.

Die neue Regelung erlaubt es, ein Programm unter Einsatz technischer Mittel in ein Computersystem der betroffenen Person einzubringen, um dadurch Nachrichten und Informationen zu überwachen, die verschlüsselt über ein Kommunikationsnetz oder einen Dienst der Informationsgesellschaft gesendet, übermittelt oder empfangen werden. Voraussetzung hierfür ist, dass dies zur Vorbeugung eines verfassungsgefährdenden Angriffs erforderlich erscheint und dass andere Ermittlungsmassnahmen aussichtslos wären oder dass die Überwachung unbedingt erforderlich ist. Bei dem verfassungsgefährdenden Angriff muss es sich um eine Straftat handeln, die mit einer Freiheitsstrafe mit einer Obergrenze von mindestens zehn Jahren bedroht ist, oder um Spionage[60].[61] Die Überwachung soll durch ein **Programm** geschehen, **welches Nachrichten und Informationen noch vor deren Verschlüsselung beziehungsweise nach deren Entschlüsselung ermittelt**.[62]

Während die ersuchte Stelle im Rahmen der Überwachung **unverschlüsselter** Nachrichten und Informationen verpflichtet ist, die angefragten Auskünfte zu erteilen und an der Überwachung von Nachrichten **mitzuwirken**, ist dies bei der **Überwachung verschlüsselter Nachrichten nicht der Fall**. **Um das Programm ohne Kenntnis der betroffenen Person einzubringen**, darf die Direktion Staatsschutz und Nachrichtendienst als zuständige Bundesbehörde technische Mittel einsetzen, nicht jedoch neue Sicherheitslücken schaffen. **Der Anbieter muss hierbei nicht mitwirken und ist auch nicht verpflichtet, bestehende Sicherheitslücken offenzuhalten.** Um das Programm aus der Ferne und dadurch ohne physischen Zugriff auf das betroffene Gerät im richtigen Computersystem einzubringen, muss sich dieses System längerfristig in der Verfügungsgewalt der betroffenen Person befinden, sodass es eindeutig identifiziert werden kann, beispielsweise über eine Seriennummer oder eine individuelle IP-Adresse. Für diese Identifizierung ist oftmals eine vorangehende Observation sowie eine **Anfrage an Betreiber öffentlicher Telekommunikationsdienste** und sonstiger Dienste erforderlich, um die **personenbezogenen Daten zu ermitteln**. Es ist jedoch verboten, in die geschützten Räume der betroffenen Person einzudringen, um das Programm zu installieren.[63]

Für eine solche Überwachung muss im Vorfeld eine **Bewilligung des zuständigen Senats des Bundesverwaltungsgerichts** eingeholt werden, wobei bei Gefahr im Verzug auch die Bewilligung durch den zuständigen Einzelrichter des Bundesverwaltungsgerichts ausreichend ist.[64] Die Bewilligung darf nur in dem Umfang und für denjenigen künftigen Zeitraum erteilt werden, der zur Erfüllung der Aufgabe voraussichtlich nötig ist. Das Gesetz begrenzt diesen Zeitraum allerdings auf **höchstens drei Monate**, wobei eine Verlängerung mit entsprechender Bewilligung möglich ist.[65] Es dürfen auch lediglich solche Nachrichten und Informationen überwacht werden, die **innerhalb dieses Umfangs und Zeitraums gesendet, übermittelt oder empfangen werden**.[66]

Noch vor Stellung des Antrags auf Bewilligung muss der oder die **Rechtsschutzbeauftragte** kontaktiert werden und ihm oder ihr drei Werktage gelassen werden, um sich zu äussern.[67] Soll ein bestimmtes **Programm zum ersten Mal eingesetzt** werden, so muss zuvor der Bundesminister oder die Bundesministerin für Inneres verständigt werden, welcher oder welche sodann der

---

60 Im Sinne des § 256 StGB.

61 § 11 Abs 1 Z 9 in Verbindung mit Z 8 Staatsschutz- und Nachrichtendienst-Gesetz (SNG) in der Fassung des Änderungsentwurfs, verfügbar unter https://www.parlament.gv.at/dokument/XXVIII/I/136/fname_1693648.pdf (30.09.2025), dortiger Art 1 Z 10.

62 136 der Beilagen XXVIII. GP – Regierungsvorlage – Erläuterungen, verfügbar unter https://www.parlament.gv.at/dokument/XXVIII/I/136/fname_1693650.pdf (30.09.2025), S. 6.

63 136 der Beilagen XXVIII. GP – Regierungsvorlage – Erläuterungen, verfügbar unter https://www.parlament.gv.at/dokument/XXVIII/I/136/fname_1693650.pdf (30.09.2025), S. 6 f.

64 § 15a Abs 1 Sätze 1, 2 SNG in der Fassung des Änderungsentwurfs, dortiger Art 1 Z 16.

65 § 15a Abs 3 Satz 1 SNG in der Fassung des Änderungsentwurfs, dortiger Art 1 Z 16.

66 § 15b Abs 1 Satz 1 Z 1 SNG in der Fassung des Änderungsentwurfs, dortiger Art 1 Z 16.

67 § 14 Abs 4 Sätze 1, 2 SNG in der Fassung des Änderungsentwurfs, dortiger Art 1 Z 13.

rechtsschutzbeauftragten Person Gelegenheit zur Äusserung binnen drei Monaten zu geben. Erst danach darf das Programm eingesetzt werden.[68]

[68] § 14 Abs 6 Sätze 1-3 SNG in der Fassung des Änderungsentwurfs, dortiger Art 1 Z 13.

B. DENMARK

Introduction and legal basis

Danish rules on electronic communication, including obligations of providers of telecommunication and communication services are laid down in the following pieces of legislation and Ministerial (executive) orders:

Legislation

Retsplejeloven (Administration of Justice Act) Chapter 71, available in Danish at https://www.retsinformation.dk/eli/lta/2017/1101.

Lovbekendtgørelse 2022-06-17 nr. 955 om elektroniske kommunikationsnet og -tjenester (Electronic Communication Act), available at https://www.retsinformation.dk/eli/lta/2025/681. An un-official English version of the Act (updated until 2022) is available on the website of the Agency for Digital Government at https://en.digst.dk/media/zqweipgu/act-on-electronic-communications-networks-and-services_oct2022.pdf

Ministerial orders

Bekendtgørelse 2022-03-29 nr. 380 om generel og udifferentieret registrering og opbevaring af oplysninger om en slutbrugers adgang til internettet, available at Bekendtgørelse om generel og udifferentieret registrering og opbevaring af oplysninger om en slutbrugers adgang til internettet
Bekendtgørelse 2022-03-29 nr. 381 om generel og udifferentieret registrering til og med den 29. marts 2023 og opbevaring til og med den 29. marts 2024 af trafikdata, available at https://www.retsinformation.dk/eli/lta/2022/381
EU law

The Danish legal instruments implement the requirements in a number of EU law instruments, in particular:

> Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code
>
> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
>
> (Repealed) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

Study on Data retention law in the Nordic countries

The Nordic council conducted a recent study in English entitled Data Retention Law in the Nordic Countries. This study, available at https://pub.norden.org/temanord2024-532/temanord2024-532.pdf, provides detailed information, inter alia, on the obligations of service providers to retain data and obligation to disclose data to law enforcement authorities. You'll find the relevant parts of the Study annexed to this report.

1. Does Denmark have different categories of telecommunication providers that are similar to those of the telecommunication service providers (Anbieter von Fernmeldediensten, FDA) and providers of derived communications services (Anbieter von abgeleiteten Kommunikationsdiensten, AAKD) in Swiss law?

Danish law does not clearly distinguish between providers of telecommunication services and providers of number-independent interpersonal communications (so-called NI-ICS services) and there is some ambiguity as to what extent the Danish data retention rules encompass NI-ICS. This is discussed in the Study on Data retention law in the Nordic countries (see p. 52 ff. or the Annex below).

2. What surveillance and information obligations do telecommunication service providers have in Denmark?

Providers (*Udbyder)69* of telecommunication services have an **obligation to provide information when this is requested by law enforcement authorities**. They also must assist the police in carrying out the measure.70 They have no obligation to provide information *sua sponte*. This obligation extends to NI-ICS services if it concerns the provider's own internet-based phone service. As concluded in the Study on Data Retention Law in the Nordic Countries regarding storage obligation and the type of data stored:

> The data listed in points 10 to 13 concern the provider's own internet-based phone service (IP-telephony). Such service is possibly an NI-ICS. This entails that the Danish data retention rules encompass NI-ICS in so far as the service is made available by a provider under Danish jurisdiction.[71]

The main rules for providing information upon request are laid down in Chapter 71 of Retsplejeloven (Administration of Justice Act, hereafter Rpl.). There are different categories of data, such as collection of data related to electronic communication (*teleoplysning*)) and extended collection of traffic data, i.e., traffic data from cell masts in a geographical area (*udvidet teleoplysning*)[72]

The conditions under which law enforcement authorities lawfully can request the provision of the information are regulated in Rpl. §§ 781 to 786.

According to Rpl. § 781, interference with the confidentiality of communications (*indgreb i meddelelseshemmeligheden*) is only permissible if there are "specific reasons" ("*bestemte grunde*") to assume that messages are submitted to or from the suspect by use of the electronic communications service identified by the police. Moreover, the measure must be considered of crucial importance ("*af afgørende betydning*") to the investigation.

There is also a requirement that the offense in question is of a serious nature: Access to "traffic and location data" (Rpl. § 781 a) can be obtained if the investigation concerns an offence with a **prescribed penalty of imprisonment for three years or more**. The general criminality condition of three years is

---

69 Udbyder is defined in the Electronic Communication Act as "a person who, for commercial purposes, makes products, electronic communications networks or services covered by this Act available to others."

70 Lovbekendtgørelse 2024-11-05 nr. 1160 Retsplejeloven, section 786.

71 Data Retention Law in the Nordic Countries, p. 50. The Study is available at https://pub.norden.org/temanord2024-532/temanord2024-532.pdf (17.06.2025).

72 Lovbekendtgørelse 2024-11-05 nr. 1160 Retsplejeloven, section 780.

supplemented with a list of offences with a lower level of punishment (Rpl. § 781 first para., no. 3) and offences regulated in § 81 a of the Criminal Code (Rpl. § 781 a).

As regards procedures and safeguards, the key requirements have been summarised in the Study on Data Retention Law in the Nordic Countries (p. 41) as follows (my emphasis in bold):

> Decision of *teleoplysning* [collection of data related to electronic communication] and *udvidet teleoplysning* [extended collection of traffic data, i.e., traffic data from cell masts in a geographical area] shall be **made by the court** (a decision supported by reasons (kendelse)) (rpl. § 783). The decision shall specify the communication number, location etc., and must determine the period for which the interference may be applied. The **period must be "as short as possible, not exceeding 4 weeks**", though with a possibility for renewal, which also must be decided by the court (rpl. § 783 third para.). The police may make the decision should the purpose otherwise be compromised. A court review must be obtained within 24 hours (rpl. § 783 [fourth] para.). A secret defence lawyer shall be appointed (rpl. § 784). The lawyer has a right to be present at court meetings regarding the case and have access to the case documents (rpl. § 785). E-com providers have an obligation to assist the police in carrying out the coercive measure (rpl. § 786).73

3. How does the law in Denmark regulate data retention?

The current provisions on data retention by telecommunication service providers are laid down in Chapter 71 of Rpl. The rules aim to ensure that retained data are available to the police to the widest extent possible within the framework of EU law. Since a legal reform in 202274, the law provides for an obligation of *targeted* data retention (Rpl. §§ 786 b to 786 d). Alongside that, there is an obligation of *general, undifferentiated* data retention of certain kinds of data (Rpl. § 786 e and 786 f).

Rpl. § 786 e general undifferentiated data retention to protect national security

Rpl. § 786 e allows, subject to order of the Minister of Justice, for general undifferentiated data retention to **protect national security**. Such order was given by the Minister of Justice already when the provision entered into force (30 March 2022).75 The retention period is maximum **one year.**

The **obligation concerns providers "*udbydere*".** They are defined in the Electronic Communication Act as "a person who, for commercial purposes, makes products, electronic communications networks or services covered by this Act available to others."

The data concerned is "trafikdata", which covers a large number of different kinds of data (see the Study on Data retention law in the Nordic countries p 49, or below in the Annex).

Rpl § 786 f general undifferentiated data retention

Under this provision, providers ("*udbydere", see* definition above*)* have an **obligation of general and undifferentiated registration and storage of information about an end user's access to the Internet**. The retention period is maximum **one year.**

---

73 The Study is available at https://pub.norden.org/temanord2024-532/temanord2024-532.pdf (17.06.2025).

74 Following a legal reform in 2022, Danish law abolished the previous rules that imposed a general statutory obligation on providers to indiscriminately register and store data for a period of one year.

75 Bekendtgørelse 2022-03-29 nr. 381 om generel og udifferentieret registrering til og med den 29. marts 2023 og opbevaring til og med den 29. marts 2024 af trafikdata.

The data covered is **"end user's access to the Internet"** - which is a concept **more limited than "trafikdata"** referred to in rpl § 786 e. (see the Study on Data retention law in the Nordic countries p 51, or below in the Annex). Essentially, it is limited to identify the person who used an internet connection at a certain point of time.[76]

Statutory obligation to retain certain kinds of data on a general, undifferentiated basis are thus limited to the conditions set out in Rpl. § 786 e and 786 f. Data retention in other instances may be *ordered* for limited periods of time provided that specific conditions are fulfilled. Data retention may, depending on the provision and data in question, be ordered by the National Police Authority *(Rigspolitiet)*, the District Court, or the Minister of Justice.

However, it should be stressed that the **Minister of Justice makes use of the possibility under Rpl. § 786 e** to order general undifferentiated data retention **to protect national security**. Since the data concerned is so-called "trafikdata", which covers a large number of different kinds of data, **providers' data retention obligations are currently substantial**. The type of data concerned is listed in the Minister of Justice's order.77

4. How does the law regulate the retention of boundary data ("Randdaten")?

There is no data referred to as "boundary data" in the Danish legislation. A distinction is made of the retention so-called "trafikdata" and data on "end user's access to the internet" (see previous question).

5. How long must providers in Denmark retain data?

Data retained according to rpl § 786e (general undifferentiated data retention to protect national security), which includes so-called "trafikdata", must be stored for one year.

The data referred to in rpl § 786 f (general undifferentiated data retention), which covers data on the end user's access to the Internet, must also be stored for one year.

6. Rules regarding the removal of encryption

The legal situation as regards access of law enforcement authorities to encrypted information is rather complex. The legislation aims to be technologically neutral which makes it difficult to translate what some obligations means in technical terms, such as "removal of encryption". To our understanding, there is no obligation for telecommunication providers to remove encryption that they do not have the "keys" to.[78] More generally, Danish law does not require private actors to implement backdoors or

---

76 See government Ordinance Bekendtgørelse 2022-03-29 nr. 380 om generel og udifferentieret registrering og opbevaring af oplysninger om en slutbrugers adgang til internettet.

77 See Bekendtgørelse 2025-03-28 nr. 325 om generel og udifferentieret registrering af trafikdata fra og med den 30. marts 2025 til og med den 29. marts 2026 og opbevaring til og med den 29. marts 2027 available at Bekendtgørelse om generel og udifferentieret registrering af trafikdata fra og med den 30. marts 2025 til og med den 29. marts 2026 og opbevaring til og med den 29. marts 2027.

78 Retsplejeloven (Administration of Justice Act) Chapter 71 discussed above. See also L. Højlund Christensen *et al.,* Lovbekendtgørelse 2024-11-05 nr. 1160 Retsplejeloven, Karnov Kommentar 2025, commentary to section 786 f.

provide encryption keys.[79] However, further research is required to answer this question comprehensively.

In the absence of a general obligation to remove encryption it should be borne in mind that the storage obligation includes a considerable volume of metadata that can be requested by law enforcement authorities. Moreover, as discussed under question 2, law enforcement authorities have important powers as regards the interception of data.

[79] See Cybersecurity Laws and Regulations Denmark 2025 (question 8.2), available at https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/denmark (25.09.2025).

Annex

Relevant sections from the Study "Data Retention Law in the Nordic Countries – A comparative Study"[80]

5.1 Introduction

Prior to the revision in 2022, Danish law on data retention imposed a general statutory obligation on providers to indiscriminately register and store data for a period of 1 year. The revision brought about a significant change.

Current law sets out data retention provisions in Retsplejeloven (rpl.) Chapter 71 "Interferences with private communication, etc.", § 786 b to § 786 j, and provisions of access in Chapter 74 "Seizure and Production Order". The law provides for *targeted* data retention (rpl. §§ 786 b to 786 d), and *general, undifferentiated* data retention (rpl. § 786 e and 786 f). There is but one instance of a *statutory* obligation to retain data on a general, undifferentiated basis, i.e., rpl. § 786 f relating to internet access. Data retention in other instances may be *ordered* for limited periods of time provided specific conditions are fulfilled. The competence to order data retention is held by the National Police Authority *(Rigspolitiet)*, the District Court or the Minister of Justice as further specified in the provisions.
The revised rules aim to ensure that retained data are available to the police "to the widest extent possible" within the framework of EU law.

The law provides procedural safeguards guaranteeing persons whose data are retained a level of legal protection corresponding to the protection applicable to other interferences with private communication, described in Section 5.3.1 (data preservation) and 5.4.6 *(teleoplysning)*.
Legal safeguards are afforded both at the stage of data registration and storage, and at the later stage when the data are accessed.

The following sections address the conditions for targeted data retention (6.2), and general, undifferentiated data retention (6.3). Then follows a description of the data to be registered and stored (6.4), and of whom that may be subject to an obligation to retain data (6.5). Finally, the procedure for accessing the data is described (6.6).

5.2 Targeted data retention orders

5.2.1 Introduction – the criminality condition

Targeted data retention of "traffic data" may be ordered for persons, communication equipment, and specific geographical areas pursuant to rpl. §§ 786 b to 786 d (each provision making it explicit that the measure is targeted *("målrettet")).* The purpose is to combat serious crime. The provisions apply a criminality condition closely linked to the one applicable to *teleoplysning*. Consequently, aside from generally requiring an offence of a certain seriousness as determined by the statutory level of punishment, they include the offences already described in Section 5.4.6.

5.2.2 Data retention targeting convicted persons

Retention of "traffic data" may be ordered for persons *convicted* of serious crime (§ 786 b first para.). The rationale is that once discharged from prison such persons may be at risk of resuming criminal activity, besides that they might have a criminal social network. It is assumed that registration and storage of traffic data related to such persons "on occasion" might afford the police a possibility to use the data when investigating into "possible criminal connections" *("eventuelle kriminelle forbindelser")* that these persons might have. This could be helpful in the investigation and prosecution of serious crime.

---

80 Sunde, I.M. (2024) Data Retention Law in the Nordic Countries: A Comparative Study. The Nordic Council of Ministers. TemaNord 2024:532, available at https://pub.norden.org/temanord2024-532/temanord2024-532.pdf (10.07.2025).

The length of the registration period is related to the seriousness of the crime for which the person is convicted. Rpl. § 786 b first para. no. 1 to 3, differentiate between offences with a prescribed maximum penalty of imprisonment for at least 3, 6 or 8 years, respectively (and, in addition, less serious offences as specified in Section 5.4.6). Thus, the registration periods are,

- 3 years for a person convicted of an offence with a prescribed maximum penalty of imprisonment for at least 3 years ("a 3 year offence") (no. 1),
- 5 years for a 6 year offence (no. 2), and
- 10 years for an 8 year offence (no. 3).
-

The registration period commences when the person is discharged from prison, or in the case of a conditional sentence, from the time when the verdict became final (rpl. § 786 b second para.).
The storage period is 1 year (rpl. § 786 b fifth para.). It follows that the provider must delete data on a running basis one year from the date when the data were registered.

Order of data retention related to convicted persons is issued by the National Police Authority *("Rigspolitiet")* (rpl. § 786 b first para.). The person whose data are registered shall not be notified (rpl. § 786 b seventh para.).

5.2.3 Data retention targeting communication equipment and persons

Rpl. § 786 b third para., no. 1 to 4, provide for retention of "traffic data" with respect to communication equipment and persons that *have been subject to* interception or *teleoplysning* as mentioned in rpl. §§ 780 first para., no. 1 or 3. Furthermore, data may be retained regarding persons who are or have been *in possession* of such communication equipment. Data may also be retained regarding communication equipment that was *contacted* by communication equipment subject to interception or *teleoplysning*.
It is not required that the persons whose data may be retained were prosecuted or convicted.

The registration period is 1 year. The period commences from the date when the interception or *teleoplysning* terminated, and the date at the end of that year is a *fixed* date. Thus, registration may follow immediately upon the termination of the coercive measure, and last for a year. Should the registration start later, it may not continue for a full year, only for the remaining part of it (rpl. § 786 b fourth para).

The storage period is 1 year after registration (rpl. § 786 b fifth para.).
Order of data retention related to communication equipment and persons is issued by the National Police Authority *("Rigspolitiet")* (rpl. § 786 b third para.) The person whose data are registered shall not be notified (rpl. § 786 b seventh para.).

5.2.4 Data retention targeting geographical area

Pursuant to rpl. § 786 c, retention of "traffic data" may be ordered for geographical areas, however, in this case with the limitation that "traffic data related to fixed telephony including the providers' own internet phone service" shall not be retained.

First paragraph states that data retention may be ordered for the parts of providers' networks necessary to cover geographical areas measuring 3 kilometres x 3 kilometres. For the area in question, it must be demonstrated that the number of serious crimes *reported* to the police, or the number of inhabitants *convicted* for serious crime, amount to at least 1,5 times the average national rate calculated as the average over the last three years. The offences in question must have a prescribed maximum penalty of imprisonment for at least 3 years or, be one of those mentioned in Section 5.4.6.
Second paragraph states that data retention may be ordered with respect to "special security critical areas" *("særlig sikringskritiske områder")*. The provision sets out a list exemplifying such areas, e.g., the residences of the royalty and the prime minister, embassies, police premises, prisons, bridge-, tunnel- and ferryway connections, large traffic intersections, border gateways, bus terminals, train and metro stations, military areas, high-risk enterprises involving storage of substances causing risk of fire or explosion, poisonous substances or substances causing environmental risk *("kolonne 3 virksomheder"),* and public airports.

The provision does not fix a maximum period for the registration of data.
The storage period is limited to 1 year (third para.).

Order of data retention related to geographical areas is issued by the National Police Authority *("Rigspolitiet")* (rpl. § 786 c first and second para.). Persons whose data are retained shall not be notified (fifth para.).

5.2.5 Data retention based on a concrete assessment

Rpl. § 786 d provides legal basis for retaining "traffic data related to communications equipment, persons or specific areas" pursuant to a concrete assessment *(konkret begrundede pålæg)*. Like rpl. § 786 c, the provision excludes "traffic data related to fixed telephony including the providers' own internet phone service" (rpl. § 786 d first para., last sentence).

Data may thus be retained if there is "reason to assume" *("grund til at antage")* that the object (i.e., the communications equipment, the person or the geographical area in question) "has connection with" *("har forbindelse til")* serious crime, i.e., offences with a prescribed maximum penalty of imprisonment for at least 3 years, or offences as mentioned in Section 5.4.6. The area does not have to be the same or be related to the geographical areas targeted with basis in rpl. § 786 c.

The provision extends the possibility of the police to gain access to traffic data at an early stage of an investigation, beyond what is provided for in § 780 first para. (3) and (4), § 781 and § 781 a, as these provisions require "specific reasons" *("bestemte grunde")* to assume that messages to and from the suspect are transmitted by use of the targeted communication equipment, and that the measure is "crucial" *("af afgørende betydning")* to the investigation. In contrast, pursuant to § 786 d, it is sufficient that there is "reason to assume" that the object "has connection with" serious crime. However, in contrast to decisions about *extended/teleoplysning* the police do not get immediate access to the data, as access requires an additional procedure, see Section 6.6.

The rationale for rpl. § 786 d is that at the time when the measure is needed "there will not necessarily exist a concrete suspicion that a person has committed or will commit a crime, nor that a crime was or will be committed in a specific geographical area."

This is further supplemented with the observation that "a retention order may therefore also be issued in respect of specific areas when the police has reason to believe that it has a connection to the planning of serious crime."

A data retention order with basis in rpl. § 786 d must be issued by the court, as the conditions necessitate broad assessments. Such wide scope for discretion should be exerted by an independent judge. This sets the provision apart from the provisions dealt with in the preceding sections, where data retention is ordered by the National Police Authority, the reason being that the provisions apply objective conditions that make the law more foreseeable to the citizens.

The court order must specify the registration period which must be "as short as possible, not exceeding 6 months". The period may be renewed (by court order) for a maximum of 6 months each time. The order shall specify the targeted person, communication equipment or geographical area (rpl. § 786 d second para).

The storage period is 1 year (third para).
Persons whose data are retained are entitled to the same procedural safeguards as applicable to *extended / teleoplysning,* described in Section 5.4.6 (rpl. § 786 d, fourth para.).

5.3 General, undifferentiated data retention

5.3.1 Introduction

The law provides for general undifferentiated data retention in two instances as per rpl. §§ 786 e and 786 f. The first instance necessitates the execution of an order, whereas the other concerns an obligation that follows directly from the legal provision itself.

5.3.2 National security

To protect national security the Minister of Justice may order providers to perform general, undifferentiated data retention (rpl. § 786 e). The obligation is comprehensive (no exception for data related to fixed telephony or the provider's own internet phone service).

The material condition is that there are "concrete circumstances sufficient to cause an assumption that Denmark is faced with a serious threat against national security that must be deemed as real and present or foreseeable" *("tilstrækkelig konkrete omstændigheder, der giver anledning til at antage, at Danmark står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig.")*

The assessment shall be performed at regular intervals to ensure that both national and international circumstances are taken into consideration.

Moreover it shall be based on several elements, such as

- analysis of criminal cases, pending and concluded, concerning offences laid down in Chapter 12 and 13 in the Criminal Code (offences against national security, the constitution and higher central institutions, and terrorism);
- unclassified analyses by the Intelligence Service of the Police *(PET)*, the Military Intelligence Service, and the Cybersecurity Centre; and
- the annual Assessment of the Terrorist Threat against Denmark by the Centre of Terrorism Analysis *("Vurderingen af Terrortruslen mot Danmark» (VTD)).*

The registration period is 1 year as a maximum (rpl. § 786 e second para). The preparatory works emphasize that the period must in any case not be longer than "strictly necessary."
The data shall be stored for 1 year (rpl. 786 e third para).

Prior to the order, the Minister of Justice shall have negotiated with the Minister of Commerce (rpl. § 786 e first para.).

Rpl. § 786 e was activated already at the date when the revised law entered into force (30 March 2022), by decision of the Minister of Justice after negotiation with the Minister of Commerce (BEK no. 381). The retention period was set to 1 year commencing 30 March 2022 ending 29 March 2023. The data shall be stored until 29 March 2024. Attached to the decision is an assessment that includes information as listed in the preparatory works, see above. The assessment was thus made publicly available.

5.3.3 Internet access

Providers have a general, undifferentiated obligation to register data related to "end-users'" access to internet (rpl. § 786 f). The data shall be stored for 1 year.

Data about internet access are deemed to be "of crucial importance" *("helt afgørende")* to the investigation of a broad range of crime, in particular crime committed "in the digital domain", notably child sexual abuse, distribution of illicit images, as well as hacking cases which have been on the rise recent years. Generally, circumstances indicate that the police have a need to - unambiguously and efficiently - be able to determine the identity of an end-user's identity on basis of data about internet access.

In contrast to the other provisions, rpl. § 786 e does not require the crime to be serious.
The reason is that the data to be retained do not expose the person's private life as such, as they do not concern the servers accessed in the internet session, or third parties the person has communicated with. The data only identify the person who used an internet connection at a certain point in time (see also Section 6.4.2). The interference is thus deemed to be rather small. The data however may be vital to the investigation of all types of crime.

Further rules about retention of internet access data are set out in BEK no. 380. The regulation specifies the providers comprised by the regulation (Chapter 1 "Scope" §§ 1-3), the data to be registered and by whom (Chapter 2 §§ 4-7) and finally states that a contravention of the regulation is a criminal offence punishable with a fine, and that criminal liability may be incurred also by corporations (§ 8).

5.4 The data to be registered

5.4.1 Traffic data

The data to be registered and stored by the providers are referred to as "traffic data" (rpl. §§ 786 b to 786 e) and "data about an end-user's access to internet" (rpl. § 786 f). "Traffic data" are further specified in a regulation containing thirteen categories of data, set out with legal basis in rpl. § 786 fourth para. The data categories are reiterated in the preparatory works (see below).
The categories encompass more data than often regarded as traffic data, such as A- and B number, time, and duration of a communication. It also includes *location data* related to mobile telephony (point 6), as well as name and address of subscribers and registered users (points 8 and 12), the latter often known as *subscriber data*.
The list set out in the regulation is exhaustive. Data not on the list are not "traffic data" and may not be comprised by a retention order even if they are generated in the provider's service, for instance for network error detection. An example is signal data, i.e., data documenting a connection between a mobile phone and a cell mast when the mobile phone is turned on but not in use by the owner.
Such data may still be subject to a preservation order.

"Traffic data":
Data related to fixed and mobile telephone networks, as well as to communication by SMS, EMS and MMS:

1. Source number (A-number), and name and address of the subscriber or registered user,
2. Receiving number (B-number), and name and address of the subscriber or registered user,
3. Change of receiving number (C-number), and name and address of the subscriber or registered user,
4. Receipt of received messages,
5. The identity of the devices used in the communication (e.g., IMSI- or IMEI-numbers),
6. The cell or those cells a mobile phone is connected to at the beginning and end of a communication, as well as precise data about the associated cell masts' geographical or physical location at the time of the communication, and
7. The time when the communication begins and ends.

Data related to the providers' own e-mail services:

8. Sender's e-mail address, and
9. Recipient's e-mail address.

Data related to the provider's own internet-based phone services (IP-telephony):

10. The allocated user identity ("User-ID"),
11. The User-ID and phone number allocated to communications performed in a public electronic communication network,
12. Name and address of the subscriber or registered user, to whom an IP-address, a user identity or a phone number was allocated at the time of the communication, and
13. The time when the communication begun and ended.

The data listed in points 10 to 13 concern the provider's own internet-based phone service (IP-telephony). Such service is possibly an NI-ICS. This entails that the Danish data retention rules encompass NI-ICS in so far as the service is made available by a provider under Danish jurisdiction.

Although not explicitly stated in the legal provisions, the providers' obligation to retain data only concerns data "that are generated or processed in [their] network."

If data specified on the list are not generated in the provider's network, for technical or other reasons, they fall outside the scope of the obligation. The provider is not obliged still to generate and store them.

The obligation may be limited also by the scope of the legal provisions. This is the case for rpl. § 786 c (geographical areas) and 786 d (order based on a concrete assessment), both explicitly excluding traffic data about fixed telephony and providers' own internet phone services from the obligation (cf. first paragraph of both provisions).

5.4.2 Internet access data

BEK no. 380 § 4 specifies internet access data as "data that are generated or processed in providers' network" concerning:

1. The User-ID allocated to the end-user by the provider. The User-ID may be a customer number, subscriber number or similar data that identify the end-user vis a vis the internet access provider,
2. The User-ID and telephone number allocated to communications in a public electronic network. «User-ID» means identifying data allocated by the provider to the end-user when the end-user accesses the internet, including IP-address, source port number and other identifying data,
3. Name and address of the subscriber or registered user regarding whom an IP-address, a User-ID or a telephone number was allocated at the time when the internet was accessed.
4. The points in time when the internet was accessed, and the access was terminated.

As noted in Section 6.3.3, the purpose of retaining data about internet access pursuant to rpl. § 786 f, is to ensure availability of data that may identify the person who used an internet connection at a certain point in time. These data are referred to in rpl. § 786 f as "data about an *end-user's* access to internet" (italics added). "End-user" *(slutbruger)* is defined in DECA § 2, no. 3 as
a user of electronic communications networks or -services, *who on a non-commercial basis makes the said networks or services available to others* (italics added).

This could be organisations such as universities and public libraries and hospitals that offer internet access to their students, clients, patients. However, clearly the provision also aims for the possibility to identify individuals using their private internet connection, without making it available to others. In such case they are possibly to be regarded as "users", which is not a defined term in DECA § 2 (the preparatory works comment that "user" and "end-user" shall be regarded as synonyms).
Pursuant to the definitions set out in the e-kodex Directive Article 2 points 13 and 14 there is a difference though: "user" meaning a person "*using* … a publicly available electronic communications service", and "end-user" meaning a person "*not providing* … publicly available electronic communications services."

The Danish notions seems to be somewhat at odds with the e-kodex definitions.

5.5 Provider

5.5.1 The definition

The data retention provisions specify generally that the obligation to retain data is incumbent on "providers" *("udbydere")*. "Provider" is defined in DECA § 2, no. 1as
anyone who for a commercial purpose makes products, electronic communication networks or -services encompassed by DECA available to others.

The condition "for a commercial purpose" is central to the definition and means that the product, network, or service must be offered for the purpose of gaining a profit directly or indirectly.
Seemingly, the condition is easily applicable to actors providing fixed and mobile telephony. On the internet side however, the situation is a bit more complicated.

Firstly, it is not relevant whether the activity in fact generates a profit or not. For instance, a hotel offering "hot-spot" internet in the lobby, or internet or telephony in the hotel room, and does this without compensation, is still deemed to be a "provider" as the reason for offering the service is to make the hotel more attractive, thus gain a profit.

The commercial purpose is also fulfilled if the activity normally is offered for profit, even though commercial activity is not the main objective. For instance, a local municipality renting out a building to local entrepreneurs including "free" internet, is a "provider" within the meaning of DECA, therefore also within the meaning of the data retention rules.

Libraries, hospitals, universities, schools etc., offering electronic networks or services to their clients, are not deemed to do this for a commercial purpose, hence are not "providers".

Instead, they are "end-users" as explained in Section 6.4.2. To illustrate: A provider must retain data related to its own e-mail service (see Section 6.4.1, points 8 and 9). A provider is a provider within the meaning of the law only if the service is offered for a commercial purpose. With an example from a Norwegian context; the commercial e-com company Telenor that offers the e-mail service @online.no, would (pursuant to Danish regulation) have an obligation to retain data about the sender's and the recipient's e-mail address, while the University of Oslo that offers the e-mail service @uio.no, to its 33 000 students and staff members, is deemed not to have a commercial purpose and would not have to retain such data.

Furthermore, recalling that the list of traffic data includes data related to the "provider's own internet-based phone services," the question is who these providers are, specifically whether providers of NI-ICS generally are included.

The question was touched upon in Section 6.4.1, but it is possible to dig a little deeper. At the outset, to be provider of a service within the meaning of DECA § 2, no. 1, the service must be an "electronic communications service" as defined in DECA § 2, no. 9. The definition requires the service to be transmitted between "network termination points", i.e., physical end points in the electronic network (DECA § 2, no. 8). NI-ICS as defined in DECA § 2 no. 20 is not a service transmitted between physical endpoints, rather use of NI-ICS requires that internet access (a network termination end point) is already available. This prompts the question whether a provider of an internet-based phone service as mentioned in the list of "traffic data" set out in Section 6.4.1, must offer the service *in addition* to a service that is transmitted between network termination points such as fixed and mobile telephony, or internet access. In such case, only a small number of NI-ICS providers are "providers" within the meaning of the data retention rules.

5.5.2 Internet Access Providers

As rpl. § 786 f concerns retention of internet access data, a "provider" within the meaning of the provision must mean one who provides an internet access service. Reg. 380 sets out further details. Firstly, § 1 makes clear that the term "provider" shall have the same meaning as in DECA § 2, no. 1., entailing that the condition "for a commercial purpose" applies. However, transmission of radio- or TV-programs (over the internet) is positively excluded from the regulation (§ 2). This is in line with the e-kodex Directive Article 2 no. 4, which excludes services exercising editorial control over electronic content (see Section 5.1.3).

Organisations that provide internet access to their members are not comprised by the obligation unless the number of members is 100 or more (§ 3). Organisations set up to manage apartment complexes could be covered by this rule.

If several providers register the same data, at least one of them shall do this as an obligation under rpl. § 786 f (§ 5). A provider may enter into an agreement with another provider or a third party about registration and storage of internet access data on its behalf (§ 6).

5.6 Access to retained data

The police may gain access to retained data by use of production order pursuant to the provisions set out in rpl. Ch. 74 Seizure and Production Order *(beslaglæggelse og edition).* A production order may compel a person who is not a suspect to provide access to an object in his or her custody, if the object is deemed to be relevant as evidence in a criminal investigation (rpl. § 804 in conj., with § 801 first para., no. 1). The offence under investigation must be subject to public prosecution *(offentlig påtale)*. A production order with legal basis in rpl. § 804 must be issued by a court (rpl. § 806 second para.).
However, in respect of "traffic and location data" retained pursuant to rpl. §§ 786 b to 786 e, rpl. § 804 a is the legal basis for a production order. This provision makes the conditions and safeguards applicable to udvidet/ teleoplysning) applicable to police access to retained traffic and location data as well, see rpl. § 804 a in conj., with §§ 805 and 806. These conditions and safeguards were explained in Section 5.4.6. The decision is made by the court. The police may make the decision should the purpose otherwise be compromised. In such case a judicial review must be obtained within 24 hours (rpl. § 806 fourth para.). Importantly, to access traffic and location data the investigation must concern an offence with a prescribed maximum penalty of no less than three years. This substantially raises the threshold compared to production order issued pursuant to rpl. § 804. The

regulation of access to traffic and location data is also in alignment with the conditions for access to preserved data (rpl. § 786 a) (see Section 5.3.1).

Rpl. § 804 b concerns production order regarding data that "identify an end-user's access to electronic communications networks or-services." The provision is applicable to retained static internet access data, IMEI and IMSI numbers. The order may be issued by the police. This differs from §§ 804 and 804 a, according to which the court must make the decision. However, similar to the condition set out in rpl. § 804, the investigation must concern an offence liable to public prosecution. Dynamic data about internet access, such as dynamic IP-addresses and source port numbers may not be accessed on basis of rpl. § 804 b, instead the procedure prescribed in rpl. § 804 must be applied, entailing that a court order is needed as opposed to an order of the police.

This extra safeguard was deemed necessary as identifying relevant dynamic data might not be as straightforward as for static data. The difference in legal procedure for access to static and dynamic IP-addresses is however not easily discerned from the text of the legal provisions themselves. Also data not subject to retention such as signal data must be accessed pursuant to § 804. As the provider's possession of the data is unrelated to any duty to retain, such data fall outside the scope of rpl. §§ 804 a and 804 b.

C. FRANCE

1. La France dispose-t-elle de différentes catégories de fournisseurs de télécommunications qui sont similaires à celles des fournisseurs de services de télécommunications (Anbieter von Fernmeldediensten, FDA) et des fournisseurs de services de communication dérivés (Anbieter von abgeleiteten Kommunikationsdiensten, AAKD) en droit suisse ?

En droit français, il existe une distinction à peu près comparable entre les opérateurs et les fournisseurs de télécommunication :

- Les **opérateurs** ont un double rôle d'exploitation du réseau et de fourniture de service de communications électroniques[81]. La jurisprudence a ainsi précisé que pouvaient être considérés comme des opérateurs de télécommunication **Orange**[82](anciennement France Telecom), **Bouygues**[83] et **SFR**[84] et **Free**[85].
- Les **fournisseurs**, quant à eux, pourraient plus correspondre à la notion de fournisseurs de services de télécommunication dérivés en droit suisse, car ils éditent ou adaptent le système d'exploitation d'équipements terminaux, éditent ou adaptent tout autre logiciel contrôlant l'accès aux fonctionnalités desdits équipements[86], assurent la mise à disposition de contenus, services ou applications relevant de la communication au public en ligne, éditent un service de communication au public en ligne, ou assurent le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature »[87]. La jurisprudence a ainsi précisé que pouvait être considéré comme des fournisseur : **Youtube**[88].

2. A quelles obligations de surveillance et d'information les fournisseurs de services de télécommunication sont-ils soumis en France ?

Depuis l'entrée en vigueur de l'ordonnance portant transposition en droit français du Code des communications électroniques européen, les opérateurs et fournisseurs sont soumis aux mêmes obligations :

- Respect du secret des correspondances (article L. 32-3), respect des conditions de confidentialité et de neutralité au regard des messages transmis et des informations liées aux communications (article L.33-1) et respect de la protection des données à caractère personnel.
- S'assurer des conditions de permanence, de qualité, de disponibilité, de sécurité et d'intégrité du réseau et du service (article L. 33-1).
- Absence de discrimination entre opérateurs et entre opérateurs et fournisseurs pour l'acheminement du trafic et de l'accès à leurs services (article L.32-1, III, 3°).

---

81 Article L.32, 15°, Code des postes et des communications électroniques.

82 CA Chambéry, 1ere chambre, 17 décembre 2024, n°22/00551.

83 CA Douai, 2e chambre, 16 novembre 2023, n°21/03145.

84 CA Versailles, chambre sociale 4-3, 17 juin 2024, n°21/03055.

85 Cour de cassation, civile, Chambre civile 1, 20 mars 2024, 22-23.115.

86 Article L.32, 10°, Code des postes et des communications électroniques.

87 Article L.32, 23°, Code des postes et des communications électroniques.

88 Tribunal judiciaire de Paris, 9 novembre 2023, 21/06216.

- Exercice d'une concurrence effective et loyale entre les exploitants de réseau et les fournisseurs de services de télécommunication (article L. 32-1, III, 1°).
- Respect de l'ordre public et des obligations de défense et de sécurité publique (article L.32-1, II, 7°) et prendre les mesures nécessaires pour acheminer gratuitement les appels d'urgence.
- **Fournir les informations ou documents** demandés par le **ministre** chargé des communications électroniques ou l'**Autorité** de régulation des communications électroniques, des postes et de la distribution de la presse, et **notifier ces mêmes autorités en cas d'incident de sécurité** ayant un impact significatif sur leur fonctionnement.
- respect du principe de neutralité vis-à-vis du contenu des messages transmis (article L.32-1,II, 6°).
- **Fournir des documents** intéressant une **procédure pénale** : Les données issues d'un système informatiques peuvent être interceptées par des officiers de police judiciaire autorisés par le juge des libertés et de la détention, à la requête du procureur de la République. Ces **réquisitions sont possibles selon les différentes phases de la procédure pénale** (enquête de flagrance[89], enquête préliminaire[90], ou information judiciaire[91]). Si le législateur parle de "documents", "y compris ceux issus d'un système informatique ou d'un traitement de données nominatives", la Chambre criminelle admet à ce titre la communication de données de connexion[92]. Les données de connexion peuvent contenir, par exemple, des données d'identification, des données de trafic, ou encore des données de localisation.
- **Coopérer** face aux mesures d**'interception de données** d'un système informatique ordonnées dans le cadre d'une **procédure pénale** : En matières criminelle et correctionnelle, l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications sont prévues sous l'autorité et le contrôle du juge d'instruction, « lorsque les nécessités de l'information judiciaire l'exigent »[93]. En cas de délit puni d'une peine d'emprisonnement commis par la voie des communications électroniques sur la ligne de la victime, l'interception ne peut intervenir que sur cette ligne, et à la demande de la victime[94]. Les opérateurs et fournisseurs de services de communications électroniques sont tenus de répondre à ces demandes **dans les meilleurs délais**[95].

Le non-respect de ces obligations peut mener au **blocage** d'un site par l'ARCOM, Autorité de régulation de la communication audiovisuelle et numérique [96]. Cette autorité peut même demander le blocage d'un site aux fournisseurs d'accès à internet sans l'intervention d'un juge, après une mise en demeure et un délai d'un mois dans le cas de contenus pornographiques fourni à des personnes mineures[97].

3. Comment la loi française régit-elle la conservation des données ?

La loi française fixe un **principe général d'effacement ou d'anonymisation** des données par les opérateurs de communications électroniques. Ce processus vise à rendre impossible toute identifica-

89 Articles 60-1 et 60-2, CPP.

90 Articles 77-1-1 et 77-1-2, CPP.

91 Articles 99-3 et 99-4, CPP.

92 Cass. crim., 22 novembre 2011, n° 11-84.308.

93 Article 100, CPP.

94 Article 100, CPP.

95 Article L871-2, Code de la sécurité intérieure.

96 Tribunal administratif de Paris, 5e section - 4e chambre, 15 avril 2025, n° 2506972.

97 Article 10-1, Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

tion des individus au sein de jeux de données, ce qui est irréversible. Lorsque cette anonymisation est effective, les données ne sont plus considérées comme des données personnelles au sens de la loi.

En revanche, ces mêmes **operateurs sont tenus de conserver certaines catégories de données**:

- Pour les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique et de la sauvegarde de la sécurité nationale :
  - les informations relatives à l'identité civile de l'utilisateur[98] (nom, prénom, date et lieu de naissance ou raison sociale et nom et prénom, date et lieu de naissance de la personne agissant en son nom lorsque le compte est ouvert au nom d'une personne morale ; adresses postales associées ; adresses de courrier électronique de l'utilisateur ; numéros de téléphone[99])
  - les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte (identifiant utilisé ; pseudonymes utilisés ; données destinées à permettre à l'utilisateur de vérifier son mot de passe ou de le modifier[100]) ainsi que les informations relatives au paiement[101] (type de paiement utilisé ; référence du paiement ; montant ; date, heure et lieu en cas de transaction physique[102]).

- Pour les besoins de la lutte contre la criminalité et la délinquance grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de la sécurité nationale :
  - les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés[103] (identifiant de la connexion ; identifiant attribué à l'abonné ; adresse IP attribuée à la source de la connexion et port associé ; types de protocoles utilisés pour la connexion au service et pour le transfert des contenus[104]).

- Pour des motifs tenant à la sauvegarde de la sécurité nationale, lorsqu'est constatée une menace grave, actuelle ou prévisible, contre cette dernière (par décret du Premier ministre) :
  - certaines catégories de données de trafic et de données de localisation (dates et heure de début et de fin de la connexion ; caractéristiques de la ligne de l'abonné ; identifiant attribué par le système d'information au contenu, objet de l'opération ; nature de l'opération ; date et heure de l'opération ; identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni[105]).
- les données relatives aux bulletins de paie des salariés[106]
- les images de vidéo protection[107]
- certaines données médicales.[108]

98 Article L.34-1, II bis du code des postes et télécommunication.

99 Article R10-13, I, Code des postes et des communications électroniques.

100 Article R10-13, II, Code des postes et des communications électroniques.

101 Article L.34-1, II bis du code des postes et télécommunication.

102 Article R10-13, III, Code des postes et des communications électroniques.

103 Article L.34-1, II bis du code des postes et télécommunication.

104 Article R10-13, IV, Code des postes et des communications électroniques.

105 Article R10-13, V, Code des postes et des communications électroniques.

106 Article L. 3243-4 du code du travail.

107 Article L. 252-3 du code la sécurité intérieure.

108 Code de la santé publique.

Les personnes qui fournissent au public des services de communications électroniques doivent établir des procédures internes permettant de répondre aux demandes de données des autorités compétentes.

Les données conservées et traitées portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux. Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications.
Les autorités disposant de l'accès légal aux données peuvent émettre une injonction de conservation rapide pour la prévention et la répression de la criminalité, de la délinquance grave et des manquements graves.

Certaines données considérées comme sensibles ne peuvent être recueillies ou utilisées, sauf si la personnes concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée) : les données relatives à la santé des individus, la vie sexuelle ou l'orientation sexuelle, l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses, philosophiques ou l'appartenance syndicale, les données génétiques et biométriques utilisées aux fins d'identifier une personne de manière unique.

4. Comment la loi francaise régit-elle la conservation des métadonnées (« Randdaten ») ?

Lors de l'audience solennelle de rentrée du tribunal de grande instance du 22 janvier 2018, François Molins, procureur de la République, mettait en garde contre un arrêt de la CJUE (aff. C-203/15, *Tele2 Sverige AB*) et pointait l'importance de l'obtention de métadonnées (données de connexion et de localisation d'un téléphone portable trouvé dans une poubelle devant le Bataclan) afin d'identifier les terroristes plus rapidement et stopper leur course après l'attentat du Bataclan.

Le droit français adopte une **position ambivalente face à la jurisprudence de la Cour de justice de l'Union européenne** (CJUE), notamment depuis l'arrêt *La Quadrature du Net* (CJUE, 6 oct. 2020), qui interdit la conservation généralisée et indifférenciée des métadonnées. Bien que le Conseil d'État ait reconnu l'incompatibilité de certaines dispositions françaises avec le droit de l'Union (CE, 24 avr. 2021, *French Data Network*), **il continue d'admettre, au nom de la sécurité nationale, une conservation étendue des métadonnées**.

Suivant la logique de l'arrêt *Arcelor*, le Conseil d'État donne la primauté au bloc de constitutionnalité sur le droit européen dans certains cas, en invoquant des objectifs à valeur constitutionnelle comme la prévention des atteintes à l'ordre public ou la lutte contre la criminalité. Ainsi, il autorise la conservation généralisée des métadonnées lorsqu'une menace grave et réelle est identifiée, ainsi que la conservation ciblée des données, même si elles ont été initialement collectées à d'autres fins.

Le Conseil constitutionnel, de son côté, a censuré partiellement l'ancien article L. 34-1 du Code des postes et des communications électroniques (CPCE), en relevant une atteinte disproportionnée aux libertés en raison de l'imprécision du texte (Cons. const., 25 févr. 2022). Toutefois, cette censure reste sans véritable effet, car elle porte sur un texte abrogé, et certaines dispositions inconstitutionnelles restent valides, ce qui entre en contradiction avec le droit de l'Union.

Les détails concernant les types de données conservées et la durée de conservation de ces données sont traités dans le reste de cette note.

5. Combien de temps les fournisseurs doivent-ils conserver les données en France ?

La durée de conservation légale des données par les opérateurs, les fournisseurs et les hébergeurs dépend du type de données traitées, avec une durée de conservation variant de 1 mois à 20 ans.

- **Vingt ans** à compter de la date du dernier séjour du patient dans l'établissement médical ou de la dernière consultation externe en son sein pour les dossiers médicaux[109].
- **Dix ans** à compter de la date du décès du patient si la personne titulaire du dossier décède moins de dix ans après son dernier passage dans l'établissement pour le dossier médical[110].
- **Cinq ans** à compter de la fin de validité de son contrat[111] pour les informations relatives à l'identité civile de l'utilisateur, pour les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique et de la sauvegarde de la sécurité nationale.
- **Cinq ans** pour double des bulletins de paie des salariés ou les bulletins de paie remis aux salariés sous forme électronique par l'employeur[112].
- **Un an** à compter de la fin de validité de son contrat ou de la clôture de son compte[113] pour les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte ainsi que les informations relatives au paiement, pour les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique et de la sauvegarde de la sécurité nationale.
- **Un an** à compter de la connexion ou de l'utilisation des équipements terminaux[114], pour les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés, pour les besoins de la lutte contre la criminalité et la délinquance grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de la sécurité nationale.
- **Un an** pour certaines catégories de données de trafic et de données de localisation, pour des motifs tenant à la sauvegarde de la sécurité nationale, lorsqu'est constatée une menace grave, actuelle ou prévisible, contre cette dernière (par décret du Premier ministre).
- **Un mois** pour les images de vidéo protection[115].

Les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée[116].

---

109 Article R1112-7, code de la santé publique.

110 Article R1112-7, code de la santé publique.

111 Article L.34-1, II bis du code des postes et télécommunication.

112 Article L. 3243-4 du code du travail.

113 Article L.34-1, II bis du code des postes et télécommunication.

114 Article L.34-1, II bis du code des postes et télécommunication.

115 Article L. 252-3 du code la sécurité intérieure.

116 Article 5, Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD).

6. Règles relatives au déchiffrement des données

Le droit français définit le **moyen de cryptologie** comme « tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité » (article 29, Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique). Une **convention de déchiffrement** s'entend de tout moyen logiciel ou de toute autre information permettant la mise au clair d'une donnée transformée par un moyen de cryptologie, que ce soit à l'occasion de son stockage ou de sa transmission. Il en résulte que le code de déverrouillage d'un téléphone mobile peut constituer une clé de déchiffrement si ce téléphone est équipé d'un moyen de cryptologie (Cryptologie (convention de déchiffrement) : déverrouillage d'un téléphone portable – Cour de cassation, ass. plén. 7 novembre 2022 – D. 2022. 1968).

La loi n° 2004-575 pour la confiance dans l'économie numérique du 21 juin 2004 pose le principe de la **liberté d'utilisation des moyens de déchiffrement** (art. 30). Elle détermine les obligations des personnes fournissant des prestations de cryptologie et les sanctions encourues en cas de non-respect de ces obligations.

Ainsi, la **fourniture, le transfert, l'importation et l'exportation de moyens de cryptologie** assurant exclusivement des **fonctions d'authentification ou de contrôle d'intégrité** sont **libres** (article 30). Toutes les autres activités sont soumises à une **déclaration préalable** auprès du Premier ministre et à une **obligation d'information**. Les informations que le fournisseur ou la personne procédant au transfert ou à l'importation doit transmettre au Premier ministre incluent une description des caractéristiques techniques de ce moyen de cryptologie et le code source des logiciels utilisés.

La gestion des déclarations et la délivrance des déclarations relatives aux moyens et prestations de cryptologie sont assurées par **l'Agence nationale de la sécurité des systèmes d'information** (article 4, Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information »).

Un décret fixe une **liste d'opérations dispensées de formalité préalable** (Annexe 1, Décret n°2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie), et une **liste d'opérations soumises à déclaration préalable** (Annexe 2, Décret n°2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie). Les **autres opérations** sont soumises à **autorisation préalable**.

Des débats législatifs sont en cours sur l'intégration de dispositions législatives interdisant l'utilisation « de dispositifs techniques visant à affaiblir volontairement la sécurité des systèmes d'information », c'est-à-dire les **backdoors**. Ainsi, l'amendement N° 1 rect. Quinquies interdisant l'usage des backdoors a été adopté au Sénat lors de la séance du 12 mars 2025, mais à une très faible majorité, dans le projet de loi Résilience des infrastructures critiques et renforcement de la cybersécurité. Ce texte est désormais examiné par la Commission spéciale chargée d'examiner le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité de l'Assemblée nationale, qui auditionne actuellement des acteurs du domaine. Par exemple, un docteur en cryptographie et fondateur de la société de communication électronique Olvid a soutenu l'adoption de cet amendement lors de son audition du 9 juillet 2025 devant cette Commission spéciale.

6.1 Quels types de données doivent être déchiffrées ?

L'article 434-15-2 du code pénal **incrimine le refus**, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, **de remettre ladite convention aux autorités judiciaires** ou de la mettre en œuvre, sur les réquisitions de ces autorités. Si le refus est opposé alors que la remise ou la mise en œuvre de la convention **aurait permis d'éviter la commission** d'un crime ou d'un délit ou d'en limiter les effets, la **peine** prévue est **aggravée**. L'article 132-79 du code pénal prévoit que, lorsqu'un moyen de cryptologie a été utilisé **pour préparer ou commettre** un crime ou un délit, ou **pour en faciliter la préparation ou la commission**, le **maximum de la peine** privative de liberté encourue est **relevé**.

6.2 Qui doit déchiffrer les données ?

Selon l'article 230-1 du Code de procédure pénale, le déchiffrement des données saisies ou obtenues au cours de l'enquête ou de l'instruction peut être confié à **toute personne physique ou morale qualifiée**, désignée par le procureur de la République, la juridiction d'instruction, l'officier de police judiciaire (sur autorisation du procureur ou du juge d'instruction), ou la juridiction de jugement saisie de l'affaire. Si la personne désignée est une personne morale, son représentant légal doit soumettre à l'agrément de l'autorité compétente le nom des personnes physiques chargées de réaliser techniquement le déchiffrement. Ces personnes doivent, sauf exceptions, **prêter serment** conformément aux dispositions du code.

Cela inclut les **prestataires de services de cryptologie** visant à assurer une fonction de confidentialité (article L871-1, Code de la sécurité intérieure), les **opérateurs** et les **fournisseurs de services de communications électroniques** (article 871-2, CSI).

6.3 Quels contenus doivent être communiqués aux autorités dans un format déchiffré ?

Les autorités doivent pouvoir avoir accès à toute donnée cryptée susceptible d'avoir été utilisée pour **préparer, faciliter ou commettre** un crime ou un délit, ou qui aurait pu **permettre d'éviter la commission** d'un crime ou d'un délit ou d'en limiter les effets.

6.4 Existe-t-il des exceptions au principe de déchiffrement des données ?

Oui. Le Conseil constitutionnel, dans sa décision n° 2018-696 QPC, a jugé que l'obligation de remettre une clé de déchiffrement (article 434-15-2 du Code pénal) n'est conforme à la Constitution que si la personne concernée a effectivement connaissance de la clé et que la réquisition émane d'une autorité judiciaire. Cette obligation ne doit pas contraindre une personne à s'auto-incriminer : elle ne peut viser qu'à permettre le déchiffrement de données déjà existantes, indépendantes de sa volonté, et non à obtenir des aveux. Ainsi, une personne ne peut être sanctionnée pour refus de déchiffrement ni si elle ignore la clé, ni si la demande porte atteinte à ses droits fondamentaux, comme **le droit au silence, la présomption d'innocence ou le respect de la vie privée.**

Le **secret professionnel** peut également constituer un motif légitime de refus de remettre une clé de déchiffrement, notamment pour les professions protégées comme les avocats, médecins ou journalistes. Conformément à l'article 60-1 du Code de procédure pénale et à la jurisprudence, ce refus est recevable si les données concernées sont directement couvertes par le secret, en particulier lorsqu'elles relèvent de l'exercice du droit de la défense ou d'une activité protégée. Toutefois, cette protection n'est pas automatique : le juge peut en vérifier la légitimité. Si le secret est invoqué abusivement ou si les données chiffrées ne sont pas réellement protégées par ce secret, la personne

peut être contrainte de collaborer. De même, si la clé permet d'accéder à des données personnelles ou étrangères à l'activité protégée, l'obligation de déchiffrement peut s'appliquer.

D. GERMANY

In Deutschland regelt das **Telekommunikationsgesetz** (TKG)[117] die Pflichten von Telekommunikationsanbietern. In diesem wurden auch die Vorgaben der Richtlinie 2018/1972 umgesetzt.[118] Weitere relevante Regelungen finden sich in der Telekommunikations-Überwachungsverordnung (TKÜV)[119], im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)[120] sowie in der Technischen Richtlinie zur Umsetzung gesetzlicher Massnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften (TR TKÜV)[121].

1. Kategorien an Telekommunikationsdienstleistern (Anbieter von Fernmeldediensten (FDA), Anbieter von abgeleiteten Kommunikationsdiensten)

Seit Dezember 2021 gelten die Definitionen des EKEK/EECC.[122] Interpersonelle Telekommunikationsdienste (Art. 2 Nr. 5 EKEK bzw. § 3 Nr. 24 TKG) werden unterteilt in sogenannte **nummerngebundene** (**NB-ICS**, § 3 Nr. 37 TKG)[123] und **nummernunabhängige** (NI-ICS, § 3 Nr. 40 TKG)[124] interpersonelle Telekommunikationsdienste[125]. Entscheidendes Abgrenzungskriterium zwischen den beiden Unterkategorien ist die Art der Nummernnutzung.

In seinen Vorschriften über Auskunftsersuchen der Sicherheitsbehörden nennt das TKG als **Adressaten der Vorschriften** «nummerngebundene interpersonelle Telekommunikationsdienste, Internetzugangsdienste oder Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen,» sowie «Anbieter von im Voraus bezahlten Mobilfunkdiensten» und «[Erbringer] nummernun-

---

117 Verfügbar unter https://www.gesetze-im-internet.de/tkg_2021/index.html (22.05.2025).

118 Vgl. Gesetz zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts (Telekommunikationsmodernisierungsgesetz), BGBl. I 2021, S. 1858 ff., verfügbar unter http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1858.pdf (01.07.2025).

119 Verfügbar unter https://www.gesetze-im-internet.de/tk_v_2005/index.html (22.05.2025).

120 Verfügbar unter https://www.gesetze-im-internet.de/ttdsg/ (22.05.2025).

121 Verfügbar unter https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/TechnUmsetzung110/Downloads/TR_TKUEV_Ausgabe_8.3.pdf?__blob=publicationFile&v=5 (22.05.2025).

122 BGBl. 2021 I, S. 1858 ff., verfügbar unter http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1858.pdf (22.05.2025).

123 Nummerngebundene interpersonelle Telekommunikationsdienste (*number-based interpersonal communications services*, kurz: NB-ICS) stellen eine Verbindung zu öffentlich zugeteilten Nummerierungsressourcen her oder ermöglichen die Kommunikation mit Nummern nationaler oder internationaler Nummerierungspläne (§ 3 Nr. 37 TKG).

124 Nummernunabhängige interpersonelle Telekommunikationsdienste (*number-independent interpersonal communications services*, kurz: NI-ICS) stellen weder eine Verbindung zu öffentlich zugeteilten Nummerierungsressourcen her noch ermöglichen sie die Kommunikation mit Nummern nationaler oder internationaler Nummerierungspläne (§ 3 Nr. 40 TKG).

125 Es handelt sich also in erster Linie um sogenannte Online-Kommunikationsdienste wie E-Mail, Messenger, Videotelefonie oder Videokonferenz; vgl. Bundesnetzagentur, Einstufung von NI-ICS, verfügbar unter https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/Onlinekommunikationsdienste/NIICS/start.html (23.06.2025).

abhängige[r] interpersonelle[r] Telekommunikationsdienste». Letzteres umfasst insbesondere Erbringer von öffentlich zugänglichen E-Mail-Diensten sowie Messenger-Anwendungen.[126]

Die **Anbieter von NI-ICS** unterliegen gegenüber der Bundesnetzagentur nicht der Meldepflicht. Die Bundesnetzagentur nimmt jedoch grundsätzliche **Einstufungsprüfungen**[127] für auf den deutschen Markt ausgerichtete NI-ICS vor und unterrichtet die Anbieter dieser Dienste über die Einstufung sowie über die neuen gesetzlichen Pflichten für NI-ICS nach dem TKG. Die regulatorischen Verpflichtungen nach dem TKG gelten für NI-ICS insbesondere im Bereich öffentliche Sicherheit wie beispielsweise der Auskunftspflicht für bestimmte Nutzerdaten und der Beantwortung von Auskunftsersuchen.[128]

2. Überwachungs- und Informationspflichten

Die **rechtliche Grundlage für Überwachungsmassnahmen** findet sich nicht in den eingangs genannten Gesetzen und Verordnungen, sondern in anderen Gesetzen, wie insbesondere § 100a Strafprozessordnung (StPO)[129], § 3 Artikel 10-Gesetz[130], § 72 Zollfahndungsdienstgesetz (ZFdG)[131], § 51 Bundeskriminalamtgesetz (BKAG)[132] sowie in den Polizei- und Ordnungsgesetzen der Bundesländer. Überwachungsmassnahmen durch Strafverfolgungsbehörden (§ 100a StPO) bedürfen einer richterlichen Anordnung, welche bei Gefahr im Verzug durch eine Anordnung durch die Staatsanwaltschaft ersetzt werden kann. Letztere muss jedoch innerhalb von drei Werktagen durch das Gericht bestätigt werden.[133]

Bei Massnahmen zur Überwachung von Telekommunikation unterscheidet das Gesetz im Hinblick auf Erbringer öffentlich zugänglicher Telekommunikationsdienste[134] zwischen solchen, die eigene Telekommunikationsanlagen betreiben[135], einerseits und solchen, die sich eines anderen Betreibers einer Telekommunikationsanlage bedienen, andererseits. Demnach müssen **Betreiber von Telekommunikationsanlagen** ab dem Zeitpunkt der Betriebsaufnahme auf eigene Kosten technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Massnahmen zur Überwachung der Telekommunikation vorhalten und unverzüglich umsetzen.[136] Bestimmte Telekommunikationsanlagen sind von diesen Vorgaben jedoch ausgenommen, unter anderem solche, an welche nicht mehr als 10'000 Nutzer angeschossen sind.[137] **Erbringer von öffentlich zugänglichen Telekommunikationsdiensten, die sich hierfür eines anderen Betreibers einer Telekommunikationsanlage bedienen**,

---

126 Vgl. Bundestag, Drucksache 19/26108 vom 25.01.2021, S. 367; siehe auch J. Ferner, in J. Graf (Hrsg.), BeckOK StPO mit RiStBV und MiStra, 55. Ed., München 2025, § 172 TKG, Rn. 9.

127 Siehe ausführlich zur Einstufung als NI-ICS auch Bundesnetzagentur, Hinweispapier zur Einstufung von nummernunabhängigen interpersonellen Telekommunikationsdiensten (NI-ICS), 2025, verfügbar unter https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/OnlineKom/NICS/Hinweispapier_NIICS.pdf?__blob=publicationFile&v=3 (29.09.2025).

128 Bundesnetzagentur, Nutzung von Online-Kommunikationsdiensten in Deutschland, 2023, verfügbar unter https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/OnlineKom/befragung_lang23.pdf?__blob=publicationFile&v=4 (22.05.2025), S. 10.

129 Verfügbar unter https://www.gesetze-im-internet.de/stpo/index.html (22.05.2025).

130 Verfügbar unter https://www.gesetze-im-internet.de/g10_2001/ (22.05.2025).

131 Verfügbar unter https://www.gesetze-im-internet.de/zfdg_2021/ (22.05.2025).

132 Verfügbar unter https://www.gesetze-im-internet.de/bkag_2018/ (22.05.2025).

133 § 100e Abs. 1 StPO.

134 Im Sinne des § 3 Nr. 44 i.V.m. Nr. 61 und 1 TKG.

135 Im Sinne des § 3 Nr. 60 i.V.m. Nr. 8 TKG.

136 § 170 Abs. 1 Nr. 1 TKG.

137 § 3 Abs. 2 S. 1 TKÜV.

müssen sich hingegen lediglich bei der Auswahl des Betreibers vergewissern, dass dieser die Anordnungen zur Überwachung der Telekommunikation umsetzen kann.[138]

Die **Weitergabe von Teilnehmerdaten** erfolgt meist automatisiert über die Bundesnetzagentur und dies ohne richterlichen Beschluss.[139] Bei Bedarf ist auch eine manuelle Abfrage möglich.[140]

3. Speicherung von Daten

Sowohl nummerngebundene als auch nummernunabhängige interpersonelle Telekommunikationsdienste sind **verpflichtet, zwecks der möglichen Identifizierung der Anschlussinhabenden Bestandsdaten zu erheben und zu speichern**.[141] Fahrlässige oder vorsätzliche Verstösse gegen diese Pflicht stellen eine Ordnungswidrigkeit dar[142] und werden mit einem Bussgeld von bis zu 300'000 Euro sanktioniert.[143]

Bei den **zu speichernden Daten** handelt es sich bei nummerngebundenen interpersonellen Telekommunikationsdiensten um 1. die Rufnummern, 2. andere vergebene Anschlusskennungen, 3. Namen und Anschrift des Anschlussinhabers, 4. bei natürlichen Personen deren Geburtsdatum, 5. bei Festnetzanschlüssen die Anschrift des Anschlusses, 6. allenfalls die Gerätenummer des überlassenen Mobilfunkgeräts sowie 7. das Datum der Rufnummernvergabe und des Vertragsbeginns.[144] Nummernunabhängige interpersonelle Telekommunikationsdienste müssen die als Nummer 1, 3, 4 und 7 genannten Daten speichern, wobei Nummer 1 dann die Kennung des Dienstes meint und Nummer 3 den Nutzer des Dienstes.[145]

4. Speicherung von Randdaten

Das deutsche Recht kennt den Begriff der Randdaten nicht. Stattdessen definiert es die sogenannten **Verkehrsdaten** als diejenigen «Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind».[146] Davon zu unterscheiden sind insbesondere die Bestandsdaten sowie die Standortdaten.

Der Begriff der Bestandsdaten meint die «Daten eines Endnutzers, die erforderlich sind für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste».[147] Es handelt sich also um die gemeinhin als Vertragsdaten bezeichneten Informationen.

---

138 § 170 Abs. 2 Nr. 1 TKG.
139 § 173 TKG.
140 § 174 TKG.
141 § 172 Abs. 1, 3 TKG.
142 § 228 Abs. 2 Nr. 49, 50 TKG.
143 § 228 Abs. 7 Nr. 3 TKG.
144 § 172 Abs. 1 S. 1 Nr. 1-7 TKG.
145 § 172 Abs. 3 TKG.
146 § 3 Nr. 70 TKG.
147 § 3 Nr. 6 TKG.

Die Standortdaten hingegen bezeichnen diejenigen «Daten, die in einem Telekommunikationsnetz oder von einem Telekommunikationsdienst verarbeitet werden und die den Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben».[148]

Die sogenannte **Vorratsdatenspeicherung**[149] bezog sich auf die Speicherung von Verkehrsdaten und wurde zuletzt im August 2023 vom Bundesverwaltungsgericht für **verfassungs- und unionsrechtswidrig** erklärt,[150] nachdem der Europäische Gerichtshof auf Vorlage entsprechend geurteilt hatte.[151] In der Folge dürfen die der Vorratsdatenspeicherung zugrundeliegenden Vorschriften bis auf Weiteres nicht angewendet werden.[152]

5. Dauer der Datenspeicherung

Die für Auskunftsersuchen der Sicherheitsbehörden zu speichernden **Bestandsdaten** müssen **nach Vertragsende gelöscht** werden, allerdings erst mit **Ablauf des auf die Vertragsbeendigung folgenden Kalenderjahres**.[153] Ein vorsätzlicher oder fahrlässiger Verstoss hiergegen stellt eine Ordnungswidrigkeit dar[154] und wird mit einem Bussgeld von bis zu 300'000 Euro sanktioniert.[155]

Eine 2015 eingeführte Regelung zur Vorratsdatenspeicherung[156] sah vor, dass nur ausgewählte Daten (keine E-Mails) gespeichert werden dürfen[157] und dies für maximal 10 Wochen, Standortdaten lediglich für maximal 4 Wochen.[158] Wie bereits unter Punkt 4. dargestellt, sind diese Regelungen zwar noch im Gesetz enthalten, wurden jedoch für verfassungs- und unionsrechtswidrig erklärt. Sie werden daher nicht mehr angewendet.

6. Vorgaben zur Entfernung von Verschlüsselungen

In Deutschland sehen die **Strafprozessordnung**[159] sowie das **Bundeskriminalamtgesetz**[160] die sogenannte «Quellen-Telekommunikationsüberwachung» («**Quellen-TKÜ**») vor. Demnach darf zur Telekommunikationsüberwachung auch mit technischen Mitteln in die informationstechnischen Systeme einer Person eingegriffen werden, sofern dies erforderlich ist, um die Überwachung und

---

148 § 3 Nr. 56 TKG.

149 Geregelt in den §§ 176-181 TKG.

150 BVerwG, Urteile vom 14.08.2023 – 6 C 6.22 und 6 C 7.22, verfügbar unter https://www.bverwg.de/de/140823U6C6.22.0 und https://www.bverwg.de/de/140823U6C7.22.0 (22.05.2025).

151 EuGH, Urteil vom 20.09.2022 – C-793/19, C-794/19, verfügbar unter https://curia.europa.eu/juris/document/document.jsf?text=&docid=265881&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1 (22.05.2025).

152 Siehe Bundesnetzagentur, Verkehrsdatenspeicherung, verfügbar unter https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/Ueberwachung_Auskunftsert/VDS_113aTKG/node.html (22.05.2025).

153 § 172 Abs. 6 TKG.

154 § 228 Abs. 2 Nr. 53 TKG.

155 § 228 Abs. 7 Nr. 3 TKG.

156 BGBl. 2015 I, S. 2218 ff., verfügbar unter http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s2218.pdf (22.05.2025).

157 § 176 Abs. 5 TKG.

158 § 176 Abs. 1 Nr. 1, 2 TKG.

159 § 100a Abs. 1 S. 2, 3 StPO.

160 § 51 Abs. 2 BKAG.

Aufzeichnung in unverschlüsselter Form zu ermöglichen. Es wird also entweder vor der Verschlüsselung oder nach der Entschlüsselung auf das System der betroffenen Person zugegriffen. Dies kann insbesondere durch Aufzeichnung oder Kopie der manuellen Tastatureingabe mittels sogenannter Key-Logger geschehen.[161]

Wer **Telekommunikationsdienste erbringt oder daran mitwirkt**, muss dem Gericht, der Staatsanwaltschaft oder den für diese tätigen polizeilichen Ermittlungspersonen beziehungsweise dem Bundeskriminalamt **die Massnahme ermöglichen und unverzüglich die erforderlichen Auskünfte erteilen**.[162] Die Massnahme selbst wird also nicht von den Erbringern der Telekommunikationsdienste durchgeführt, sondern durch die zuständigen Strafverfolgungsbehörden.[163] Die Telekommunikations-unternehmen müssen jedoch **informiert** werden und erhalten für Ihre Mitwirkung, insbesondere in Form der Auskunftserteilung, eine **Entschädigung**.[164]

Voraussetzung für eine Quellen-TKÜ ist, dass **bestimmte Tatsachen den Verdacht begründen, jemand habe eine besonders schwere Straftat begangen, versucht oder bereite eine solche vor**. Diese Tat muss auch im Einzelfall schwer wiegen und die Ermittlung von Sachverhalt oder Aufenthaltsort der beschuldigten Person muss auf andere Weise wesentlich erschwert oder aussichtslos sein.[165] Das Bundesverfassungsgericht hat die Massnahme im Juni 2025 teilweise für verfassungswidrig erklärt. Demnach darf eine Quellen-TKÜ zwar weiterhin angeordnet und durchgeführt werden, allerdings nur soweit sie an solche Straftaten anknüpft, die eine **Höchstfreiheitsstrafe von mehr als drei Jahren** androhen. Es muss sich also um besonders schwere Straftaten handeln.[166]

Zum Erfordernis der **richterlichen Anordnung** siehe bereits unter Punkt 2.

Während die Massnahme lediglich auf laufende Kommunikation beschränkt ist, wenn sie auf das Bundeskriminalamtgesetz gestützt wird,[167] **umfasst die Massnahme im Rahmen der Befugnisse auf Grundlage der Strafprozessordnung sowohl die gerade stattfindende Kommunikation als auch bereits übertragene Inhalte einer abgeschlossenen Kommunikation, allerdings nur Daten frühestens ab dem Zeitpunkt der Anordnung**. Für ältere Daten wie insbesondere weiter zurückliegende Messenger-Mitteilungen muss eine sogenannte **Online-Durchsuchung**[168] angeordnet werden, für welche die Voraussetzungen strenger sind.[169] So reicht für eine Online-Durchsuchung insbesondere nicht aus, dass die Person verdächtigt wird, eine Tat vorzubereiten.[170] Im Rahmen einer Quellen-TKÜ muss jeder Einsatz technischer Mittel protokolliert werden, insbesondere mit Bezeichnung des

---

161 J. Graf, in J. Graf (Hrsg.), BeckOK StPO mit RiStBV und MiStra, 56. Ed., München 2025, § 100a StPO, Rn. 126.

162 § 100a Abs. 4 S. 1-3 StPO; § 51 Abs. 6 S. 1, 2 BKAG.

163 J. Graf, in J. Graf (Hrsg.), BeckOK StPO mit RiStBV und MiStra, 56. Ed., München 2025, § 100a StPO, Rn. 130; A. Hartmann, in D. Dölling *et al.* (Hrsg.), Gesamtes Strafrecht, 5. Aufl., Baden-Baden 2022, § 100a StPO, Rn. 15 f.; C. Rückert, in H. Kudlich (Hrsg.), Münchener Kommentar zur StPO, 2. Aufl., München 2023, § 100a, Rn. 237 f.

164 § 23 Justizvergütungs- und -entschädigungsgesetz (JVEG, verfügbar unter https://www.gesetze-im-internet.de/jveg/__23.html (02.10.2025)) in Verbindung mit § 51 Abs. 6 S. 3 BKAG.

165 § 100a Abs. 1 S. 1 Nr. 1-3 StPO.

166 Bundesverfassungsgericht (BVerfG), Beschluss vom 24.06.2025 – 1 BvR 180/23, verfügbar unter https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2025/06/rs20250624_1bvr018023.html (29.09.2025).

167 § 51 Abs. 2 S. 1 Nr. 1 BKAG.

168 Im Sinne des § 100b StPO.

169 J. Graf, in J. Graf (Hrsg.), BeckOK StPO mit RiStBV und MiStra, 56. Ed., München 2025, § 100a StPO, Rn. 143.

170 § 100b Abs. 1 Nr. 1 StPO.

technischen Mittels und Angaben zur Identifizierung des betroffenen informationstechnischen Systems und der daran vorgenommenen Veränderungen.[171] Die Anforderungen an die Software zur Durchführung einer Quellen-TKÜ ist in der Standardisierenden Leistungsbeschreibung festgelegt, welche von den Sicherheitsbehörden des Bundes und der Länder 2012 entwickelt und 2017 modernisiert wurde.[172]

171 J. Graf, in J. Graf (Hrsg.), BeckOK StPO mit RiStBV und MiStra, 56. Ed., München 2025, § 100a StPO, Rn. 149.

172 Standardisierende Leistungsbeschreibung für Software zur Durchführung von Massnahmen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung, 05.10.2018, verfügbar unter https://www.bka.de/SharedDocs/Downloads/DE/Sonstiges/standardisierendeLeistungsbeschreibungQuellenTKUE.pdf?__blob=publicationFile&v=10 (29.09.2025).

E. RUSSIAN FEDERATION

Overview

In the Russian Federation, interactions between the telecommunications sector and state investigative and security agencies are governed by various **general laws** concerning the legal status of these agencies, as well as **special legislation**, such as Federal Law No. 126-ФЗ of 7 July 2003 "On Communications" (hereafter referred to as the "Communications Law") and Federal Law No. 149-ФЗ of 27 July 2006 "On Information, Information Technologies and Information Protection" (hereafter referred to as the "Information Law").

The general laws applicable to all entities are as follows:

- Criminal Procedure Code of 2001[173], which classifies the monitoring and recording of conversations (Art. 186) and the obtaining of information about connections between subscribers and/or subscriber devices (Art. 186.1) as investigative actions. These are procedural measures established by law aimed at gathering evidence and establishing the circumstances of a criminal case during a preliminary investigation. The Code defines the procedure for implementing these measures, including the requirement for investigators to obtain a court order. This order is binding on all state authorities, local government bodies, public associations, officials, other individuals and legal entities and must be strictly enforced throughout the Russian Federation (Art. 392, para. 1). Along with the general duty to implement a court order, the Code also prescribes the communications service provider to provide the investigator with the demanded information as it becomes available, but at least once a week, throughout the entire period of such an investigative action as obtaining information about connections between subscribers and/or subscriber devices (Art. 186.1 para. 4);
- Federal Law No. 144-ФЗ of 12 August 1995 "On Operational-Investigative Activities", lists the following as operational-investigative measures (i.e. measures established by law and carried out by authorised bodies for the purpose of detecting, preventing and investigating crimes, as well as collecting evidence): obtaining information; monitoring postal items, telegraph and other communications; listening to telephone conversations; obtaining information from technical communication channels; and obtaining computer information (Art. 6). Operational-investigative activities that restrict the constitutional rights of individuals and citizens to privacy in correspondence, telephone conversations, postal and telegraph communications, and the inviolability of the home are permitted based on a court order (Art. 8, para. 2). The law's primary impact on individuals is to compel them to adhere to the officials' directives only. Lawful requests by officials of bodies conducting operational-investigative activities are binding on the individuals and legal entities to whom such requests are made (Art. 15, para. 3). The law does not mention any specific individual obligations in the context of our interest. Operational-investigative measures may also be carried out in the context of mutual legal assistance to a foreign state[174].

At the same time, the **Communications Law** is in force. It **establishes the legal basis for communications-related activities** in the Russian Federation and territories under its jurisdiction. It

---

173 Hereinafter, regulatory acts are cited as of 21 July 2025 from the "Regulatory Legal Acts in the Russian Federation" database of the Ministry of Justice of the Russian Federation, located at http://pravo.minjust.ru/.

174 There is currently no special regulatory act governing the interaction between the telecommunications sector and state investigative and security agencies in the field of mutual legal assistance requests.

also **defines the powers of state authorities** in this field, as well as the **rights and obligations of individuals** engaged in such activities.

The Communications Law regulates the establishment and operation of all communications networks and facilities, the use of the radio frequency spectrum, and the provision of telecommunications and postal services within Russian territory and other territories under Russian jurisdiction. Regarding telecoms providers operating outside the Russian Federation in accordance with foreign legislation, this federal law only applies to the regulation of procedures for performing work and providing telecommunications services within territories under Russian jurisdiction (Art. 3, paras 1 and 2).
The Communications Law defines a "communications provider" ("оператор связи") as a legal entity or individual entrepreneur that provides communications services. These are activities involving the reception, processing, storage, transmission or delivery of telecommunications messages or postal items[175], and are carried out based on an appropriate licence (Art. 2, para. 32). "Telecommunications" ("электросвязь") are defined as any emission, transmission or reception of signs, signals, voice information, written text, images, sounds or messages of any kind via radio, wire, optical or other electromagnetic systems (Art. 2, para. 35).

Among other things, the purpose of the law is to create conditions that meet the communications needs of state authorities, national defence, state security, and law enforcement (Art. 1). Accordingly, it imposes several specific obligations on communications providers when interacting with investigative and security authorities.

The exercise of the **right to search for, obtain, transfer, produce and disseminate information**, the application of information technologies, and the protection of information are governed by the **Information Law**. It **identifies several categories**, including the organiser of the dissemination of information on the Internet, the organiser of instant messaging services, the hosting provider, the owner of an information resource using recommendation technologies, the search engine operator, the owner of a news aggregator, the owner of an audiovisual service, the owner of a social networking service and the owner of an advertising service, and regulates their legal status. This includes imposing special obligations on certain entities – namely, on the organiser of information dissemination on the Internet, the owner of the social networking service and the hosting provider - in their interactions with investigative and security authorities.

The Information Law does not directly define its territorial scope. The general principle is that federal laws, including the Information Law, apply throughout the entire territory of the Russian Federation. The Information Law describes its subject matter as follows: it aims to regulate relations arising from the exercise of the right to search for, obtain, transfer, produce and disseminate information; the use of information technology; the protection of information. Therefore, it can be assumed that the Information Law, including the obligations provided for therein, is applicable if the search, receipt, transfer, production or dissemination of information, or the use of information technology or the protection of information take place on the territory of the Russian Federation. The nationality of those involved in the exchange of information is not legally significant in this regard.

It is precisely the obligations laid down in specific laws – the Communications Law and the Information Law – that will be disclosed below. A significant proportion of **control under these acts is exercised by a special agency: the Federal Communications Control Authority** (hereafter referred to as the "FCCA").

---

175 For the purposes of this study, we omit the postal operator. Hereafter the telecommunications provider (a legal entity or individual entrepreneur that provides services involving the reception, processing, storage, transmission or delivery of telecommunications messages) will be referred to as the "telecoms provider".

A sharp **increase in the responsibilities** of telecommunications providers is associated with the **Yarovaya Law**, as indicated in the comparative legal information provided to us with this request. Irina Yarovaya, a member of the legislature, drafted a bill on anti-terrorist measures in 2016. This bill included the imposition of additional duties on mobile operators, such as storing information about the receipt, transmission of messages for up to three years, and storing the content of messages themselves for six months. However, this law is well known namely for receiving a lot of negative publicity and for rallies which were organized against it in the country. In fact, similar measures had been introduced before: the obligation to store metadata for six months was assigned to organizers of the dissemination of information on the Internet as far back as 2014. And more amendments were made since 2016. Provisions in force as of 25 June 2025, as well as those adopted by that date but coming into effect later, will be reflected below. Information about future rules is highlighted in italics.

1. Does Russia have different categories of telecommunication providers that are similar to those of the telecommunication service providers (Anbieter von Fernmeldediensten, FDA) and providers of derived communications services (Anbieter von abgeleiteten Kommunikationsdiensten, AAKD) in Swiss law?

1.1. Telecoms provider

A key feature of a telecommunications provider ("оператор электросвязи") as defined by the Communications Law is the provision of relevant services, i.e. the reception, processing, storage, transmission, and delivery of signs, signals, voice information, written text, images, sounds, or messages of any kind via radio, wired, optical, or other electromagnetic systems on behalf of third parties under contract with them[176]. No regulatory act requires the telecoms provider to own the network; the provider may use leased networks instead[177].

The possession of a licence is a prerequisite for legal entities or individual entrepreneurs to engage in paid activities related to the provision of communications services (Communications Law, Art. 29, para. 1). The FCCA maintains a public register of licences in the communications sector[178]. There is no register of telecoms providers as such.

The telecoms provider is a person who provides telecommunications services on either public networks ("сеть связи общего пользования") and so-called separated networks ("выделенные сети связи"), i.e. networks intended for providing telecommunications services to a limited number of users or groups of users (Communications Law, Art. 14, para. 1). The **activities of a separated network provider are regulated in the same way as those of other telecoms providers**.

---

176 Explanations from the FCCA for the Volgograd Region and the Republic of Kalmykia available at https://34.rkn.gov.ru/directions/p5883/p15966/ (21.07.2025) and the Belgorod Region available at https://31.rkn.gov.ru/directions/p38042/p38043 (21.07.2025) agree regarding what they consider the provision of a telecommunications service: putting a telecommunications network into operation and concluding a contract with a subscriber or a user for the provision of relevant telecommunications services.

177 The possession of a licence is a prerequisite for legal entities or individual entrepreneurs to engage in paid activities related to the provision of communications services (Communications Law, Art. 29, para. 1). The FCCA maintains a public register of licences in the communications sector available at https://rkn.gov.ru/communication/register/license/ (21.07.2025). There is no separate register of telecoms providers as such.

178 Available at https://rkn.gov.ru/communication/register/license/ (21.07.2025).

At the same time, the Communications Law defines **technological communication networks** ("технологические сети связи") that are **designed to support organisational production activities and the management of production processes** (Art. 15, para. 1). The owners or other holders of such networks regulate their organisation themselves. These activities are **not subject to licensing** and the **legal requirements imposed on telecoms providers do not apply to owners of such networks** until they connect their networks to a public communications network to provide communications services to users for a fee.

Consequently, under the Communications Law, the telecoms provider is defined as a legal entity or individual entrepreneur that provides telecommunication services to third parties within territories under the jurisdiction of the Russian Federation. This applies to individuals of any nationality, except those involved in the reception, processing, storage, transmission or delivery of telecommunications messages within communication networks intended for organisational production activities and technological process management.

The Communications Law classifies telecoms providers into three subcategories according to their scope of activities:

Title	Definition	Particularities
Telecoms provider (Art. 2, para. 12)	A person providing communication services on the basis of an appropriate license	-
Provider with a significant position in the public communications network[179] (Art. 2, para. 11)	A telecoms provider that, together with its affiliated companies, owns at least 25% of the installed capacity in a geographically defined numbering zone or throughout Russia, or has the ability to transmit at least 25% of the traffic there	This status confers the right to set conditions (technical, economic, informational and property) for connecting other telecommunications networks to its own network in terms of using network resources and passing traffic (Art. 19, para. 3). Such providers are subject to a number of antitrust requirements and special supervision.
Universal service provider (Art. 2, para. 13)	A telecoms provider selected by the Russian Government from among those occupying a significant position in the public communications network in at least two-thirds of the Russian territories, to provide universal communication services.	Such a person enters into an agreement with the FCCA, which imposes a number of duties, including establishing collective access facilities and access points in specific localities (Art. 58, para. 2).

[179] The FCCA maintains a public register of providers with a significant position in the public communications network available at https://rkn.gov.ru/activity/connection/register/operators/ (21.07.2025).

With regard to interactions with the authorities in relation to the suppression, investigation and prevention of offences, all these individuals are bound by the same obligations, which are described in further sections of the legal opinion.

In addition, the Communications Law specifically identifies different subcategories of telecoms providers based on the nature of their services. Two of these subcategories — mobile radiotelephone service providers ("оператор подвижной радиотелефонной связи") and internet access providers ("оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет»") — have extra obligations within the scope of this study. These obligations will be disclosed in more detail below.

1.2. Organiser of information dissemination on the Internet

Of all the individuals covered by the Information Law, the entity on whom the Law places the greatest number of obligations in our area of interest is the **organiser of information dissemination on the Internet** ("организатор распространения информации в сети «Интернет»")[180]. This is a person who carries out activities to ensure the functioning of information systems and/or computer programmes that are designed and/or used for receiving, transmitting, delivering and/or processing electronic messages from internet users (Art. 10.1, para. 1). The organiser of the dissemination of information may be any person, whether natural or legal, regardless of ownership and legal form. The only criterion used to apply this status to a person is a functional criterion reflecting the content of the activity performed[181].

The FCCA maintains a public register of organisers of information dissemination on the Internet[182]. The Information Law obliges such organisers to notify the FCCA of the commencement of their activities (Art. 10.1, para. 2) that results in the entry in the register[183]. However, there are also known cases of an inclusion of such persons in the register initiated by the state itself[184]. Inclusion in this register does not determine a person's status: the obligations of an organiser of information dissemination established by law arise from carrying out the relevant activities, not from being included in the register.

A person may have both the status of a telecoms provider and that of an organiser of information dissemination[185].

However, the Information Law also provides exceptions. The obligations of an organiser of information dissemination do not apply to operators of state or municipal information systems or to communications providers who provide communications services based on an appropriate licence for

---

180 Hereafter also referred to as the "organiser of information dissemination".

181 See commentary on Art. 10.1 in S.A. Kulikova et al. *Commentary on Federal Law No. 149-ФЗ of 27 July 2006 "On Information, Information Technologies and Information Protection"*, 2020, available at https://internet.garant.ru, authorisation required (21.07.2025).

182 Available at https://97-ФЗ.rkn.gov.ru/ (21.07.2025).

183 Failure to comply is subject to administrative liability (Code of Administrative Offences of 2001, Art. 13.31, para. 1).

184 For example, the WhatsApp messenger was involuntarily included in the register: news item available at https://www.interfax.ru/russia/999951 (21.07.2025).

185 This is confirmed in a letter of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation No. П17-11798-ОГ of 17 June 2014: "If a telecoms provider carries out activities to ensure the functioning of information systems and/or programmes for electronic computers intended for, or used for, the reception, transmission, delivery and/or processing of electronic messages from internet users, that provider is considered an organiser of information dissemination on the Internet".

licensed activities. They also do not apply to citizens (natural persons) engaged in activities to ensure the functioning of information systems and/or programmes for electronic computers intended or used for the reception, transmission, delivery and/or processing of electronic messages of internet users for personal, family or household needs (Art. 10.1, para. 5)[186]. Therefore, if the telecoms provider and the organiser of information dissemination are the same entity, that entity shall only bear the obligations of a telecoms provider. It shall only be subject to the obligations of an organiser of information dissemination if and to the extent that it provides free communications services to third parties or carries out communications activities for its own needs (i.e. unlicensed activities).

Thus, for the purposes of this study, the term "organiser of information dissemination on the Internet" can be summarised as follows: It is a person who carries out activities to ensure the functioning of information systems and/or computer programmes that are designed and/or used for receiving, transmitting, delivering and/or processing electronic messages from internet users, save for operators of state and municipal information systems, telecoms providers (in scope of their licensed activities) and individuals carrying out such activities for personal, family or household purposes[187].

At the same time, the Information Law specifically distinguishes a special subcategory of organisers of information dissemination on the Internet based on the nature of their services — the organiser of an instant messaging service ("организатор сервиса обмена мгновенными сообщениями") — who has additional obligations within the scope of this study which will be disclosed in more detail below. This subcategory includes individuals involved in activities that ensure the operation of information systems and/or programmes for electronic computers designed for the exchange of electronic messages exclusively between users of these systems and/or programs, where the sender determines the recipient(s) of the electronic message and the systems and/or programs do not allow internet users to place publicly available information on the Internet (Art. 10.1, para. 4.2).

---

186 For these purposes, in its Decree No. 747 of 31 July 2014, the Russian Government has defined a list of personal, family and household needs. These include:
1) the needs of citizens related to acquiring knowledge, skills, abilities, values, experience and competence for intellectual, spiritual, moral, cultural, creative and/or professional development, and for satisfying their educational needs and interests;
2) the needs of citizens related to activities aimed at obtaining and applying new knowledge (scientific needs);
3) the needs of citizens in relation to the generation of creative output, including computer programmes and changes to them;
4) the acquisition of goods, works and services; the search for employees; and the posting of job vacancy information;
5) housekeeping, gardening and animal breeding and care;
6) obtaining information about the technical characteristics and consumer properties of goods; the quality of services; and the results of work; and
(7) the organisation of leisure activities and/or child care.

187 The Information Law also identifies the following categories of subjects: an owner of an information resource with recommendation technologies (Art. 10.2–2); an operator of a search engine (Art. 10.3); an owner of a news aggregator (Art. 10.4); an owner of an audiovisual service (Art. 10.5); an owner of an advertising service (Art. 10.7). It imposes several special duties on them that are not related to interacting with the authorities to prevent, investigate and suppress offences. However, if these subjects receive, transmit, deliver and/or process electronic messages from internet users, they may be recognised as organisers of the dissemination of information on the Internet as well. In this case, they also bear the corresponding obligations.

1.3. Owner of a social network

According to Art. 10.6, para. 1 of the Information Law, an individual is considered an "owner of a social network" ("владелец социальной сети") if that individual possesses the following characteristics simultaneously:

1) ownership of certain objects, such as a website, web page, information system or computer programme;

2) the functionality of these objects enables their users to create personal pages and distribute information in the official language of the Russian Federation, the official languages of its constituent entities or other languages spoken in the Russian Federation[188];

3) these objects (website, information system, or computer programme) allow the distribution of advertising aimed at consumers in the Russian Federation;

4) these objects are accessible to more than 500,000 internet users located in the Russian Federation within a 24-hour period.

The Information Law distinguishes social network owners as a separate category. However, these individuals also belong to the category of organisers of information dissemination, as they fully meet the criteria for this role. Accordingly, they also bear the obligations of organisers of information dissemination.

The FCCA independently identifies social networks on the Internet and maintains a register of them (Information Law, Art. 10.6, para.11)[189]. Once a social network has been included in the register, the FCCA notifies it of the applicable Russian legal requirements for such information resources (ibid., Art. 10.6, para.14).

1.4. Hosting provider

The Information Law defines this category ("провайдер хостинга") as persons who provide computing power for the permanent storage of information in an information system that is permanently connected to the Internet (Art. 10.2-1, para. 18). In previous editions, the rule covered individuals providing relevant services. However, this criterion was removed in 2023, with the focus now being placed on the activity itself rather than on the conclusion of contracts for the provision of services to third parties. In other words, the only criterion for this category of person is the function they perform.

It is conceivable that the organiser of information dissemination and the hosting provider are one and the same entity if that entity carries out both activities simultaneously. In such a case, it shall bear the obligations provided for both categories.

The hosting provider is also obliged to notify the FCCA of the commencement of its activities (Information Law, Art. 10.2-1, para. 1). Accordingly, a public register of hosting providers is maintained

188 The official language of the Russian Federation is Russian. However, more than 150 languages are spoken in Russia. The Institute of Linguistics of the Russian Academy of Sciences has been monitoring the languages of Russia for many years: project website available at https://jazykirf.iling-ran.ru/index.shtml (21.07.2025). Languages of Russia are defined as those that meet at least one of the following criteria: 1) speakers live in compact settlements (i.e. where the percentage of speakers of a given language is more than 20%); 2) speakers have lived in compact settlements for the last 100–150 years and still form a corresponding ethnic group; 3) half or more of speakers live in Russia. For example, European languages such as Bulgarian, Hungarian, Latvian, Lithuanian, Moldovan, German, Polish, Ukrainian, Finnish and Czech are included in the list of languages spoken in Russia.

189 Available at https://530-ФЗ.rkn.gov.ru/ (21.07.2025).

in Russia[190]. Inclusion in the register is not a condition for admission to carry out activities but merely records the fact of such activities. Currently, the register includes companies providing traditional hosting services, integrators, cloud providers, and telecommunications companies. *From 1 September 2025, the register will contain not only information about the provider, but also information about the persons to whom it provides computing power for the placement of information in an information system permanently connected to the Internet*.

2. What surveillance and information obligations do telecommunication service providers have in Russia?

2.1. Identification of users

Operational search measures and investigative actions are targeted in nature. The Communications Law and the Information Law therefore attach great importance to user identification, as this is an important prerequisite for subsequent targeted surveillance.

The telecoms provider is obliged to identify the subscriber when concluding a contract for the provision of communication services. This obligation does not stem directly from the Communications Law, but from the rules for providing communication services[191]. They equally stipulate that the telecoms provider must identify the person applying for the contract (verify the representative's powers), and that the contract must include subscriber information. The mandatory subscriber information is as follows: surname, first name, patronymic (if applicable), place of residence, date of birth, and details of an identity document.

The Communications Law imposes additional obligations on the mobile radiotelephone service provider:

- to identify not only the subscriber, but also users of the subscriber's communication services (if the subscriber is a legal entity or individual entrepreneur), and to verify the accuracy of the information provided about these individuals using the unified state identification and authentication system or by contacting state registers. The mobile radiotelephone service provider must then enter this information into the state information system for monitoring the performance of telecoms providers' duties (Art. 44, para. 6)[192];
- to identify the subscriber's terminal equipment and to enter information about it into the above-mentioned system if the subscriber is a foreign citizen or a stateless person (Art. 45.1, para. 3);
- to respond to requests from the operator of the unified state identification and authentication system about subscribers (Art. 45, para. 8).

According to the Information law, the identification obligation applies also to organisers of instant messaging services (Art. 10.1, para. 4.2), not to every organiser of information dissemination on the

---

190 Available at https://rkn.gov.ru/activity/connection/register/p1578/ (21.07.2025).
Interestingly, unlike the organiser of information dissemination, the hosting provider does not bear administrative liability for failing to notify the FCCA of the commencement of their activities.

191 These rules are approved by Russian Government resolutions for each type of communication. For example, the rules for the provision of telephone services were approved by Decree of the Russian Government No. 1994 of 30 December 2024.

192 Failure to comply is subject to administrative liability (Code of Administrative Offences, Art. 13.29, paras 2-5; Art. 19.7.10, para. 5).

Internet. This rule implies a specific method of user identification, namely establishing reliable information about the subscriber number of a mobile radio telephone connection[193].

At the same time, the Information Law stipulates that the hosting provider must not provide computing power for placing information in an information system permanently connected to the Internet, save for persons identified in accordance with the procedure established by the Russian Government[194] (Art. 10.2-1, para. 5). In other words, the identification obligation is also included in the hosting provider's legal status.

2.2. Special requirements for networks and means of communication

Another issue that arises prior to surveillance being carried out is the need to install special technical equipment on networks and devices. Both of the laws under consideration address this matter.

The Communications Law obliges telecoms providers to ensure the implementation of the requirements[195] for networks and communication facilities, enabling authorized state bodies engaged in operational search activities or ensuring Russia's security to carry out their assigned tasks[196]. Furthermore, ensuring compliance with requirements for networks and communication facilities for conducting operational search measures is one of the licensing requirements for this type of activity[197]. Correspondingly, telecoms providers must take measures to prevent the disclosure of organizational and tactical methods for carrying out these activities (Art. 64, para. 2).

Additionally, the Communications Law contains another provision for internet access providers: they have to ensure the installation of technical means[198] in its communication network to monitor compliance with the requirements for restricting access to information (Art. 46, para. 5).

The Information Law repeats the rule of the Communications Law relating to telecoms providers and obliges:

- organisers of information dissemination on the Internet – 1) to ensure the implementation of the requirements[199] for equipment and software and hardware used by the organiser in the information systems it operates, enabling authorized state bodies engaged in operational

193 This requirement is provided for by Decree of the Russian Government No. 1801 of 20 October 2021, which approved the rules for the identification of internet users by the organiser of instant messaging services. The organiser must both verify the use of this number by the subscriber and request confirmation of the subscriber's information from the mobile communications provider.

194 Rules for the identification and/or authentication of persons who apply to a hosting provider for obtaining computing power to place information in an information system permanently connected to the Internet were approved by Decree of the Russian Government No. 2011 of 29 November 2023. These rules provide for ten identification methods, including the use of the unified state identification and authentication system, a bank account, or a subscriber's number in a mobile communications network.

195 Such requirements are stipulated in ten different orders issued by the Ministry of Digital Development, Communications and Mass Media of the Russian Federation.

196 Failure to comply is subject to administrative liability (Code of Administrative Offences, Art. 13.46, para. 3).

197 Licensing requirements are listed in Decree of the Russian Government No. 2385 of 30 December 2020 "On licensing activities in the field of communication services".

198 The list of those means and the procedure for their provision are established in the FCCA's Order No. 50 of 28 February 2025.

199 Such requirements are listed in the Order of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation No. 571 of 29 October 2018.

search activities or ensuring Russia's security to carry out their assigned tasks, as well as 2) to take measures to prevent the disclosure of organizational and tactical methods for carrying out these activities (Art. 10.1, para. 4)[200], and

- hosting providers – 1) to ensure the implementation of the requirements[201] for the computing power used by the hosting provider, enabling authorized state bodies engaged in operational search activities or ensuring Russia's security to carry out their assigned tasks, as well as 2) to take measures to prevent the disclosure of organizational and tactical methods for carrying out these activities (Art. 10.2-1, para. 3).

2.3. Information obligations

The information obligations are quite similar and provided for in the law as follows:

- telecoms providers have to provide the authorized state bodies engaged in operational search activities or ensuring Russia's security with the retained information, information about users of communication services and the communication services provided to them, and other information necessary to fulfil the tasks assigned to these bodies (Communications Law, Art. 64, para. 1.1);
- internet access providers are obliged to provide information to the FCCA that allows the identification of communication facilities and user terminal equipment on the Internet (Communications Law, Art. 46, para. 5.2-1);
- organisers of information dissemination have to provide the retained information to authorized state bodies engaged in operational search activities or ensuring Russia's security, and in case of additional encoding of electronic messages, submit to the Federal Security Agency the information necessary for their decoding (Information Law, Art. 10.1, paras 3.1 and 4.1)[202];
- organisers of instant messaging services are obliged to provide information about users of the instant messaging service at the request of the authorised (since there is no specification - any) federal executive authority (Information Law, Art. 10.1, para. 4.2);
- owners of social networks have to provide information about the user of the social network at the request of the FCCA and/or the Federal Security Agency (Information Law, Art.10.6, para.1).

2.4. Other forms of interaction with authorized state bodies

Finally, there are other duties that accompany the surveillance and information obligations and are ultimately also designed to suppression, investigation and prevention of offences.

First is the obligation to terminate the provision of corresponding services. It applies to:

- telecoms providers: they have to 1) terminate the transmission of traffic on their networks containing mailings carried out in violation of the requirements of the law (Communications Law, Art. 46, para. 1); 2) terminate the provision of communication services upon receipt of a request from the body carrying out operational search activities or the FCCA, in the event of (i) non-compliance of actual users' personal data with the information stated in the

---

200 Failure to comply is subject to administrative liability (Code of Administrative Offences, Art. 13.31, para. 3).

201 Such requirements are named in the Order of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation No. 935 of 01 November 2023.

202 Failure to comply is subject to administrative liability (Code of Administrative Offences, Art. 13.31, paras 2 and 2.1).

subscription agreements, or (ii) termination of activities by a subscriber who is a legal entity or an individual entrepreneur, or (iii) for the prevention and suppression of crimes involving the use of communication networks and means of communication (Communications Law, Art. 46, para. 1; Art. 64, para. 3)[203];

- mobile radiotelephone service providers: they are obliged to stop providing communication services in cases of use of subscriber numbers by suspects, defendants and convicts in the territories of correctional institutions and pre-trial detention facilities (Communications Law, Art. 64, para. 6);
- internet access providers: they must restrict and resume access to information disseminated through the Internet in accordance with the procedure established by the Information Law (Communications Law, Art. 46, para. 5)[204];
- organisers of instant messaging services: they must limit the user's ability to transmit prohibited information at the request of the authorised federal executive authority (Information Law, Art. 10.1, para. 4.2);
- owners of social networks: they have to restrict access to a personal page at the request of the FCCA (Information Law, Art.10.6, para.1)[205].

A second associated duty is to undergo management of the network by the FCCA in extraordinary circumstances. It is imposed on telecoms providers by Art. 65.2 of the Communications Law, which stipulates that these individuals are obliged to undergo[206] management of the public communications network undertaken by the FCCA at the request of the Prosecutor General or his deputies in the event of the discovery of mass or repeated dissemination of information prohibited by the Information Law on the Internet.

Telecoms providers also have to assist the investigative authorities in carrying out investigative actions (Communications Law, Art. 64, para. 5). Such assistance is provided within the framework of criminal procedure law[207].

---

203 Failure to comply is subject to administrative liability (Code of Administrative Offences, Art. 13.2.1, para. 2).

204 Failure to comply is subject to administrative liability (Code of Administrative Offences, Art. 13.34, para. 1).

205 Failure to comply is subject to administrative liability (Code of Administrative Offences, Art. 13.50, para. 2).

206 "Undergoing" is understood to mean complying with any requirements of the governing body.
A similar process may be initiated in the event of threats to the stability, security, or integrity of the Internet or public communications networks in Russia (Communications Law, Art. 65.1). This mechanism forms part of a comprehensive set of norms concerning the so-called "sovereign Internet" (i.e. ensuring the stable, secure and holistic functioning of the Internet in Russia), within which telecom providers are assigned various obligations. In this case, hosting providers have to undergo management of the public communications network undertaken by the FCCA as well (Information Law, Art. 10.2-1, para. 4). However, as far as we understand the issue raised in the request, these duties extend beyond it.

207 See commentary on Art. 64 in T.A. Biryukova et al. *Commentary on Federal Law No. 126-ФЗ of 7 July 2003 "On Communications"*, 2015, available at https://internet.garant.ru, authorisation required (21.07.2025).
An example of such assistance in the context of an investigative action involving the obtaining of information about connections between subscribers and/or subscriber devices is provided in overview of the legal opinion.

On 1 April 2025, Federal Law No. 41-ФЗ "On the creation of a state information system for combating offences committed using information and communication technologies" was adopted. According to the act, a state information system is being created to promptly prevent, detect and suppress offences and crimes committed using information and communication technologies. *Starting from 1 March 2026, telecoms providers, organisers of instant messaging services, hosting providers, owners of social networks and owners of advertising services*[208] *will be required to interact with the system*. However, the relevant provisions and the procedure for interacting with the system have not yet been established by special by-laws. Therefore, we are unable to provide more detailed information about the obligations of those affected by the creation of this system.

3. How does the law in Russia regulate data retention?

Data retention obligation applies to both the telecoms provider and the organiser of information dissemination on the Internet.
Art. 64, para. 1 of the Communications Law stipulates that telecoms providers have to retain and store on the territory of Russia:

- information about the facts of receiving, transmitting, delivering and (or) processing voice information, text messages, images, sounds, video or other messages from users of communication services;
- text messages from users of communication services, voice information, images, sounds, videos, and other messages from users of communication services.

The first category of data is billing data. Providers retained it in order to resolve monetary disputes with clients during the reclamation period (six months), even before this obligation was introduced by law in 2016[209].

The retention and storage of the second category, which includes users' messages in various formats, is regulated by Decree of the Russian Government No. 445 of 12 April 2018. It permits the non-storage of users' information obtained from mandatory public television channels and (or) radio channels, as well as users' audio and video information obtained from audiovisual services included in the register of audiovisual services. It also stipulates, in particular, that storage shall be carried out using the telecoms provider's technical means of information storage, unless the Federal Security Agency gives consent for storage to be carried out using another telecoms provider's technical means of information storage.

---

208 Owner of an advertising service is an owner of a website and/or web page on the Internet, and/or an information system, and/or a computers programme, which are designed and/or used to organise interaction between their users for the purpose of buying, selling, exchange and/or transfer of movable and/or immovable property for use, performance of work, provision of services, search for suitable work and/or selection of necessary employees by providing their users with the opportunity to independently place advertisements in the official language of the Russian Federation, the state languages of the entities of the Russian Federation or other languages of the peoples of the Russian Federation for the sale, exchange and/or transfer for use of movable and/or immovable property, performance of work, provision of services, search for suitable work and/or selection of necessary employees, thematically grouped according to the content of such advertisements, as well as providing their users with the opportunity to independently respond to such advertisements, and access to which within 24 hours is more than one hundred thousand internet users located in the territory of the Russian Federation (Information Law, Art. 10.7, para. 1).

209 See commentary on Art. 64 in Yu.V. Volkov, Yu.N.Vakhrusheva. *Commentary on Federal Law No. 126-ФЗ of 7 July 2003 "On Communications"*, 2015, available at https://internet.garant.ru, authorisation required (21.07.2025).

Organisers of information dissemination on the Internet are obliged to retain and store on the on the Russian territory (Information Law, Art. 10.1, para. 3):

- information about the facts of receiving, transmitting, delivering and (or) processing voice information, written text, images, sounds, video or other electronic messages from internet users and information about these users *[For more information on this, see section 4 of the legal opinion]*;
- text messages, voice information, images, sounds, videos, and other electronic messages from internet users.

Similarly to the corresponding obligation of a telecoms provider, the organiser of information dissemination shall store electronic messages in the software and hardware used by this organiser in the information systems it operates, as provided for in the Russian Government's Decree No. 256 of 26 February 2022 regulating this issue. However, this act does not provide for any other possibilities. In addition, it limits the circle of users whose messages must be retained. These are users:

1) who have registered using network addresses defined by the organiser as being used within Russia;
2) who have authorised themselves using network addresses defined by the organiser as being used within Russia;
3) who have provided, during registration or when using the functions of an internet communication service (hereafter referred to as an "ICS"), an identity document issued by a Russian state authority;
4) who use devices and/or programmes for electronic computers to access an ICS that transmit geographical data (metadata) to an ICS indicating the location (temporary location) of users on the Russian territory;
5) who, when registering or using the functions of an ICS, have provided as contact information telephone numbers assigned by Russian telecommunications operators;
6) about whom the organiser has been informed by authorised state bodies carrying out operational-search activities or ensuring Russia's security that the users are located on the Russian territory.

4. How does the law regulate the retention of boundary date ("Randdaten")?

As mentioned above, Art. 10.1, para. 3 of the Information Law obliges organisers of information dissemination on the Internet to retain and store on the Russian territory information about the facts of receiving, transmitting, delivering and (or) processing voice information, written text, images, sounds, video or other electronic messages from internet users and information about these users.

The retention and storage of this data is regulated by Decree of the Russian Government No. 1526 of 23 September 2020. This act aligns with the aforementioned Decree No. 256 of 26 February 2022, in defining the scope of users whose data must be retained. And it establishes the composition of such information which includes:

1) information about the user, including the user's identifier in an ICS[210];

2) information about registration data, including:
information about the user's network addresses and ports, the network addresses and ports of an ICS used to register the user, with an indication of the exact time of registration;
information entered into an ICS by the user or the organiser of the information dissemination during user registration;
information automatically transmitted during registration to an ICS by virtue of the network protocols used by means of software installed on the user's device;
information recorded by an ICS when registering the user using other ICSs;

3) information about authorisation facts, including:
information about user authorisation facts, indicating the user's identifier in an ICS, the exact time and network addresses and ports of the user, the network addresses and ports of an ICS used for authorisation;
information recorded by an ICS when authorising the user using authorisation in other ICSs;
information automatically transmitted during authorisation to an ICS by virtue of the network protocols used by means of programs for electronic computers installed on the user's device;

4) information about changes or additions made by the user to the telephone number or email address, as well as other information specified by the user during registration;

5) information about paid services provided to the user by the organiser of the dissemination of information, indicating the exact time of their provision, the organisation providing the payment service, as well as information about the payment for such services recorded by an ICS (currency, amount, transaction number, payment system used and payment system identifiers);

6) information about the termination of registration with an ICS, indicating the user's identifier in an ICS, the exact time and network addresses and ports of the user, and the network addresses and ports of an ICS used to terminate the registration;

7) information about users recorded by a communication service if the latter provides the possibility of electronic monitoring of geolocation, reception, transmission and (or) processing of voice information, written text, images, sounds, video or other electronic messages of internet users without registration and authorisation;

8) information about the reception, transmission and/or processing of voice information, written text, images, sounds, video or other electronic messages of internet users (information about the user's network addresses and ports, the network addresses and ports of an ICS, the exact time of receipt, transmission, delivery and/or processing of electronic messages, indicating the addressees of these messages);

9) information recorded by the communication service about the organisation of the reception, transmission, delivery and (or) processing of electronic messages carried out using electronic payment system technologies, including information about the means of payment, about the monetary transactions carried out (with information about the correspondent - the payment system identifier, currency, amount, service or goods paid for (if any), other data specified during the monetary transaction), transactions carried out (indicating the payment system identifier (“electronic wallet”), the amount received or spent, other data specified during the transaction).

---

210 The organiser of an instant messaging service that is a Russian legal entity or citizen is required to store information about the identification of the users' mobile radiotelephone subscriber numbers within Russian territory (Information Law, Art. 10.1, para. 4.2).

As we can see, some of the retained information is boundary data. At the same time, however, the Decree does not stipulate any specific storage requirements for it.

5. How long must providers in Russia retain data?

Art. 64, para. 1 of the Communications Law stipulates that telecoms providers have to retain and store on the territory of Russia for three years or up to six months, depending on the type of information:

- information about the facts of receiving, transmitting, delivering and (or) processing voice information, text messages, images, sounds, video or other messages from users of communication services - for three years from the date of termination of such actions;
- text messages from users of communication services, voice information, images, sounds, videos, and other messages from users of communication services - up to six months from the end of their reception, transmission, delivery, and (or) processing;

Organisers of information dissemination on the Internet are obliged to retain and store on the on the Russian territory for three years or up to six months, depending on the type of information (Information Law, Art. 10.1, para. 3):

- information about the facts of receiving, transmitting, delivering and (or) processing voice information, written text, images, sounds, video or other electronic messages from internet users and information about these users - for one year (*starting from 1 January 2026 – for three years*) from the date of termination of such action;
- text messages, voice information, images, sounds, videos, and other electronic messages from internet users - up to six months from the end of their reception, transmission, delivery, and/or processing.

6. Rules regarding the removal of encryption

As can be seen from the section 2.3 of the legal opinion on information obligations, the law only mentions organisers of information dissemination in connection with encrypted information. These individuals have to provide the retained information to authorized state bodies engaged in operational search activities or ensuring Russia's security, and in case of additional encoding of electronic messages, submit to the Federal Security Agency the information necessary for their decoding (Information Law, Art. 10.1, paras 3.1 and 4.1). The Federal Security Agency has its Operational and Technical Measures Centre, which collects and stores encryption keys, including for other authorized agencies, to conduct operational and investigative measures to extract information from technical communication channels relating to users of communication services. These keys may be then used by agencies conducting relevant operational search activities to decrypt messages. Therefore, organisers of information dissemination are not required to decrypt messages themselves. Instead, they must provide the Federal Security Agency with the necessary encryption keys.

The Federal Security Agency's Order No. 432 of 19 July 2016, approved the procedure for organisers of information dissemination to submit information necessary for decoding electronic messages received, transmitted, delivered and/or processed by internet users. As with the Information Law, this Order does not specify the content or format of the requested information. It does not state what kind of encryption needs to be removed and what information needs to be transmitted to the responsible authorities in a readable format. These parameters shall be determined by the head (or deputy head) of the Centre when drafting the request for providing the necessary information. Encryption keys must

be provided within 10 days of the request being received, either on a magnetic medium (in the form of an electronic message by e-mail) or via granting the Centre remote access to the keys.
When considering a lawsuit challenging this Order, the Russian Supreme Court stated that the latter does not establish a different procedure for accessing such information to that enshrined in the Russian Constitution and federal laws, nor can it violate the rights of citizens and organisers of information dissemination[211]. Consequently, the provided keys may only be used under the general conditions for conducting operational search measures that restrict individuals' and citizens' constitutional rights to privacy of correspondence. This is only permitted if there is a court order to obtain computer information, substantiated by evidence of a crime being prepared, being committed, or committed using computer networks[212]. However, such a court order is not required to request encryption keys, since the Supreme Court has ruled that obtaining information necessary for decoding electronic messages is not the same as obtaining protected correspondence.
The legislation and by-laws clearly state that encryption keys must be submitted without exception. In 2017, the instant messaging service Telegram Messenger LLP challenged the decision to hold it administratively liable for failing to provide encryption keys. One of the arguments was that it was impossible to provide the requested encryption keys. It is known that the claimant justified this impossibility on the basis that neither of the two main chat organisation methods in this messenger (cloud chat or secret chat) allows for shared keys to be provided. When using the cloud method, information is stored in encrypted form and distributed across multiple servers, some of which are located outside the Russian Federation. With secret chats, one part of the key is generated on the user's device and is not stored on the organiser's equipment in any way[213]. The courts of three instances rejected the claim[214]. However, it is worth noting that they rejected this argument as one for which there is insufficient evidence, rather than because there are no exceptions to the rule (which could obviously serve as reasoning). In our opinion, that shows that in courts' view the impossibility of collecting encryption keys by an organiser of information dissemination due to the used technology (including end-to-end encryption) may serve as a circumstance precluding the need to provide decoding information. Nevertheless, we must emphasise that the current legislation does not allow for exceptions.

Conclusion

There are three main categories of entities of the field of our interest:

- telecoms providers including mobile radiotelephone service providers and internet access providers,
- organisers of information dissemination on the Internet including organisers of instant messaging services and owners of social networks[215],
- hosting providers.

Their respective obligations are summarised in the following table:

---

211 Decision of the Supreme Court of the Russian Federation No. АКПИ17-1181 of 20 March 2018.

212 M.V. Savelyeva, A.B. Smushkin. *Operational-search measures requiring judicial authorisation*, 2019, available at https://internet.garant.ru, authorisation required (21.07.2025).

213 Ibid.

214 Decision of the Moscow City Court of 22 October 2018, in case No. 4a-6215/2018.

215 *Starting from 1 March 2026, additional obligations will be imposed on owners of advertising services* ("владелец сервиса размещения объявлений") which can also be recognised as a type of organisers of information dissemination.

Category	Obligations
Telecoms provider	- when concluding a contract for the provision of communication services, to identify the subscriber; - to ensure the implementation of the requirements for networks and communication facilities, enabling authorized state bodies engaged in operational search activities or ensuring Russia's security to carry out their assigned tasks, as well as to take measures to prevent the disclosure of organizational and tactical methods for carrying out these activities; - to retain and store on the territory of Russia: information about the facts of receiving, transmitting, delivering and (or)processing voice information, text messages, images, sounds, video or other messages from users of communication services - for three years from the date of termination of such actions; text messages from users of communication services, voice information, images, sounds, videos, and other messages from users of communication services - up to six months from the end of their reception, transmission, delivery, and (or) processing; - to provide the authorized state bodies engaged in operational search activities or ensuring the security of Russia with the specified information, information about users of communication services and the communication services provided to them, and other information necessary to fulfil the tasks assigned to these bodies; - to terminate the transmission of traffic on its network containing mailings carried out in violation of the requirements of the law; - to terminate the provision of communication services upon receipt of a request from the body carrying out operational search activities or the FCCA, in the event of (i) non-compliance of actual users' personal data with the information stated in the subscription agreements, or (ii) termination of activities by a subscriber who is a legal entity or an individual entrepreneur, or (iii) for the prevention and suppression of crimes involving the use of communication networks and means of communication; - to undergo management of the public communications network undertaken by the FCCA at the request of the Prosecutor General or his deputies in the event of the discovery of mass or repeated dissemination of information prohibited by the Law on Information on the Internet; - to assist the investigative authorities in carrying out investigative actions (*starting from 1 March 2026 - to interact with the state information system for combating offences committed using information and communication technologies*)
Mobile radiotelephone service provider	- to bear above mentioned duties of a telecoms provider; - to identify not only the subscriber, but also users of the subscriber's communication services (if the subscriber is a legal entity or individual entrepreneur), as well as to verify the accuracy of the information provided about these persons using a unified state identification and authentication system or by contacting state registers, as well as to enter information

	about the subscriber, users and the contract into the state information system for monitoring the performance of telecoms providers' duties; - to identify the subscriber's terminal equipment and to enter information about it into the above-mentioned system if the subscriber is a foreign citizen or a stateless person; - to respond to requests from the operator of the unified state identification and authentication system about subscribers; - to stop providing communication services in cases of use of subscriber numbers by suspects, defendants and convicts in the territories of correctional institutions and pre-trial detention facilities
Internet access provider	- to bear above mentioned duties of a telecoms provider; - to ensure the installation of technical means in its communication network to monitor compliance with the requirements for restricting access to information; - to provide information to the FCCA that allows the identification of communication facilities and user terminal equipment on the Internet; - to restrict and resume access to information disseminated through the Internet in accordance with the procedure established by the Law on Information
Organiser of information dissemination on the Internet	- to ensure the implementation of the requirements for equipment and software and hardware used by the organiser in the information systems it operates, enabling authorized state bodies engaged in operational search activities or ensuring Russia's security to carry out their assigned tasks, as well as to take measures to prevent the disclosure of organizational and tactical methods for carrying out these activities; - to retain and store on the Russian territory: information about the facts of receiving, transmitting, delivering and (or) processing voice information, written text, images, sounds, video or other electronic messages from internet users and information about these users - for one year (*starting from 1 January 2026 – for three years*) from the date of termination of such action; text messages, voice information, images, sounds, videos, and other electronic messages from internet users - up to six months from the end of their reception, transmission, delivery, and/or processing; - to provide the retained information to authorized state bodies engaged in operational search activities or ensuring the security of Russia; - in case of additional encoding of electronic messages, submit to the Federal Security Agency the information necessary for their decoding
Organiser of an instant messaging service	- to bear above mentioned duties of an organiser of information dissemination on the Internet; - to perform user identification; - to provide information about users of the instant messaging service at the request of the authorised federal executive authority;

	- to limit the user's ability to transmit prohibited information at the request of the authorised federal executive authority (*starting from 1 March 2026 - to interact with the state information system for combating offences committed using information and communication technologies*)
Owner of a social network	- to bear above mentioned duties of an organiser of information dissemination on the Internet; - to provide information about the user of the social network at the request of the FCCA and/or the Federal Security Authority; - to restrict access to a personal page at the request of the FCCA (*starting from 1 March 2026 - to interact with the state information system for combating offences committed using information and communication technologies*)
Hosting provider	- to ensure the implementation of the requirements for the computing power used by the hosting provider, enabling authorized state bodies engaged in operational search activities or ensuring Russia's security to carry out their assigned tasks, and to take measures to prevent the disclosure of organizational and tactical methods for carrying out these activities; - to undergo management of the public communications network undertaken by the FCCA (*starting from 1 March 2026 - to interact with the state information system for combating offences committed using information and communication technologies*)

F. SPAIN

1. Does Spain have different categories of telecommunication providers that are similar to those of the telecommunication service providers (Anbieter von Fernmeldediensten, FDA) and providers of derived communications services (Anbieter von abgeleiteten Kommunikationsdiensten, AAKD) in Swiss law?

Spanish law makes a distinction between two categories of providers:

- **Providers of telecommunications services** ("Prestadores de servicios de telecomunicaciones") which include persons or companies that install and/or operate electronic communications networks, the provision of electronic communications services, their associated resources and services, radio equipment, and telecommunications terminal equipment, and are regulated by Law 11/2022, of June 28, General Telecommunications Law.[216]
- **Providers of information society services and electronic commerce services** ("Prestadores de servicios de la sociedad de la información y de comercio electrónico"), which include the services that provide content transmitted via electronic communications networks and services, activities consisting of exercising editorial control over such content, and Information Society services, and are regulated by Law 34/2002, of July 11, on Information Society Services and Electronic Commerce.[217] It also includes "intermediation services," which consist of the provision of Internet access services, the transmission of data via telecommunications networks, the temporary copying of Internet pages requested by users, hosting on own servers of data, applications or services provided by others, and the provision of tools for searching, accessing, and collecting data or links to other Internet sites.

Under each of their respective regulations, these two categories of providers have different general information duties to the competent authorities for technical, economic, or statistical purposes. However, none of these regulations cover the duties to retain or pass along certain information for the purpose of criminal proceedings, mutual legal assistance, searches for missing persons, custodial sentences or measures, intelligence activities, and internal security, as considered in the Federal Act on the Surveillance of Post and Telecommunications (SPTA).

It is useful to note that in Spain, interpersonal communications services (ICS) are divided into those based on numbering (NB-ICS) and those independent of numbering (NI-ICS). The fundamental difference lies in the dependence on numbering to identify the parties involved in the communication. NB-ICS requires a telephone number to identify the caller, while NI-ICS uses other identification methods that do not depend on numbering. This distinction is included in the Law 11/2022.[218] The same Law also makes an explicit reference to the European Electronic Communications Code in this regard.[219]

---

216 Ley 11/2022, de 28 de junio, General de Telecomunicaciones, available at: https://www.boe.es/eli/es/l/2022/06/28/11/con (02.07.2025).

217 Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, available at: https://www.boe.es/eli/es/l/2002/07/11/34/con (02.07.2025)

218 Ley 11/2022, Art. 67 and Anexo II, Definiciones Nos. 72 and 73.

219 Ley 11/2022, Disposición adicional quinta. Referencia a servicios de comunicaciones electrónicas en otras normas.

2. What surveillance and information obligations do telecommunication service providers have in Spain?

In Spain, the lawful interception of communications is regulated by the Organic Law 13/2015, of October 5, amending the Criminal Procedure Act to strengthen procedural guarantees and regulate technological investigation measures.[220] This Act modified the Spanish Criminal Procedure Act (CPA).[221]

The amended CPA text regulates various matters concerning surveillance in several chapters of its Title VII. According to EU regulations, lawful interception basically consists of passive measures that provide access and delivery of a subject's telecommunications and call associated data to law enforcement agencies,[222] like the real-time interception of a communication when it takes place ("wiretapping") or accessing stored information (excluding stored content, e.g. metadata).

It is important to note that the CPA applies to telecommunication service providers in general, and it does not consider a special category for "providers of derived communications services". As the CPA does not define what a telecommunication service provider is, one could rely on the definitions described in Section 1 above of providers of telecommunications services ("Prestadores de servicios de telecomunicaciones"), and providers of information society services and electronic commerce services ("Prestadores de servicios de la sociedad de la información y de comercio electrónico"). The latter should include apps providers such as WhatsApp, Proton, Threema or the like.

2.1 Interception of telephone and telematic communications

Article 18.3 of the Spanish Constitution guarantees the secrecy of communications, particularly postal, telegraphic, and telephone communications, except by court order. Article 55.2 of the same Constitution adds that only a law may determine the form and cases in which, individually and with the necessary judicial intervention and adequate parliamentary control, this guarantee may be suspended for specific persons in relation to investigations into the activities of armed gangs or terrorist elements. The unjustified or abusive use of these powers shall entail criminal liability as a violation of the rights and freedoms recognized by law.[223]

CPA Chapter V, Section 1 regulates the interception of telephone and telematic communications (Articles 588 ter a to 588 ter i). These measures may be ordered by a court upon request by the police, secret services, or customs authorities in connection with serious criminal proceedings, such as

---

220 Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, https://www.boe.es/eli/es/lo/2015/10/05/13/con (02.07.2025). The Organic Law 13/2015 does not have an implementing provision or ordinance, as it is, in practice, an amendment to the CPA, which does not have a single unified implementing ordinance (although some sections have implementing provisions, but not the one concerning the surveillance of telecommunications). However, there are several administrative regulations for telecommunication providers and digital infrastructures. See: Ministerio para la Transformación Digital y de la Función Pública, Legislación básica de telecomunicaciones y digital, available at: https://avance.digital.gob.es/es-es/legislacion/paginas/legislacion.aspx (02.07.2025).

221 Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, available at: https://www.boe.es/eli/es/rd/1882/09/14/(1)/con (02.07.2025).

222 Annex, Council Resolution of 17 January 1995 on the lawful interception of telecommunications, available at : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:1996:329:FULL (02.07.2025).

223 Constitución Española, available at: https://www.boe.es/eli/es/c/1978/12/27/(1)/con (20.08.2025).

terrorism or organized crime. In urgent cases, the Ministry of the Interior may order surveillance, but this must be confirmed by a court within 72 hours.[224]

Spanish secret service may also carry out surveillance if national security requires it but subject to judicial control. According to Act 2/2002 of 6 May on prior judicial control as applied to the National Intelligence Centre (CNI), the CNI may ask the operator to intercept communications in cases where the Secretary of State- Director of the CNI has obtained an authorization from a competent judge of the Supreme Court, in accordance with the specific requirements under such law, which must be confirmed by a court within 72 hours. However, in cases of justified urgency, the competent judge may confirm or deny the requested authorization with a reasoned opinion issued within 24 hours.[225]
Telecommunications service providers are required by law to maintain technical interfaces for such surveillance and to transmit data to the authorities. In the case of the interception of telephone and telematic communications there is a duty to cooperate from the providers of telecommunication services, in Chapter V, Article 588 ter e CPA:[226]

> Article 588 ter e. Duty to cooperate.
>
> 1. All providers of telecommunications services, access to a telecommunications network or information society services, as well as any person who in any way contributes to facilitating communications by telephone or any other means or system of telematic, logical or virtual communication, are obliged to provide the judge, the Public Prosecutor's Office, and the Judicial Police officers designated to carry out the measure, the assistance and cooperation necessary to facilitate compliance with the orders for the interception of telecommunications.
>
> 2. Those required to provide cooperation shall be obliged to maintain secrecy regarding the activities requested by the authorities.
>
> 3. Those obliged to comply with the above duties who fail to do so may be guilty of the offense of disobedience.

Article 58 of Law 11/2022, the General Telecommunications Law, establishes certain detailed rules regarding interception:

- Operators providing public electronic communications networks or publicly available electronic communications services must guarantee the secrecy of communications in accordance with the Spanish Constitution and must adopt the necessary technical measures.
- Operators providing public electronic communications networks or publicly available interpersonal communications services based on numbering or Internet access services (“obligated parties”) are required to carry out interceptions authorized by a court in accordance with the law at their own expense.
- Interception must be facilitated for any communication originating from or destined for the network termination point or specific terminal determined in the legal interception order, even if it is intended for information storage or processing device.[227]

---

224 Country Legal Frameworks Resource (CLFR), Provision of Real-time Lawful Interception Assistance, available at: https://clfr.globalnetworkinitiative.org/country/spain/ (02.07.2025).

225 Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, available at: https://www.boe.es/eli/es/lo/2002/05/06/2/con (02.07.2025).

226 Translated by the Swiss Institute of Comparative Law (SICL), as well as all the other legal provisions cited in this report.

227 Likewise, interception may be carried out on a known terminal with temporary location data for communications from public premises. Where there is no fixed link between the subject of the interception and the terminal used, the terminal may be determined dynamically when the subject of the interception activates it for communication by means of a personal identification code.

- Access shall be provided for all types of electronic communications available to the public, in particular, those carried out by any means of telephone and data transmission services, whether video, audio, message exchange, file exchange, or facsimile transmission. [228]
- Prior to the execution of the lawful interception order, the obligated parties must provide the authorized agent with information on the services and characteristics of the telecommunications system used by the subjects of the interception measure and, if in their possession, the corresponding names of the subscribers with their national identity document numbers, foreign identity card numbers, or passport numbers, in the case of natural persons, or the name and tax identification number in the case of legal persons.
- The obligated parties shall provide the authorized agent only the data included in the lawful interception order.
- The obligated parties shall provide the authorized agent with the information indicated in the lawful interception order (unless the characteristics of the service do not make them available) This information may include:
  a) identity or identities of the subject of the interception measure;[229]
  b) identity or identities of the other parties involved in the electronic communication;
  c) basic services used;
  d) supplementary services used;
  e) address of the communication;
  f) indication of response;
  g) cause of termination;
  h) time stamps;
  i) location information; and
  j) information exchanged through the control or signaling channel.
- Additionally, the obligated parties shall provide the authorized agent with the following data on any of the parties involved in the communication who are customers of the obligated party (unless the characteristics of the service do not make it available):
  a) identification of the natural or legal person;
  b) address at which the operator makes notifications;
  c) service account number (both the directory number and all electronic communications identifiers of the subscriber);

---

228 The access provided shall serve both for the supervision and transmission to the reception centers of the intercepted electronic communications and the information relating to the interception and shall enable the signal with which the communication is made to be obtained.

229 "Identity" means a technical label that can represent the origin or destination of any electronic communications traffic, generally identified by a physical electronic communications identity number (such as a telephone number) or a logical or virtual electronic communications identity code (such as a personal number) that the subscriber can assign to a physical access on a case-by-case basis. The obligated parties shall provide, where technically possible, the permanent identifiers necessary to attribute a service to a specific user in an unambiguous manner, as well as the identifiers of the device used for communication. If temporary identities are assigned to the user in an electronic communication, the obligated party shall, where technically possible, implement the necessary correlation measures to ensure that the permanent identities that allow the unambiguous identification of the assigned user, as well as the device used in the communication, are provided in the interception information.

d) terminal identification number;
e) account number assigned by the internet service provider; and
f) email address.

- The obligated parties must provide information on the geographical location of the terminal or network termination point from which the call originated, and that of the call's destination (unless the characteristics of the service do not make it available).[230]
- Obligated parties must have one or more interfaces ready at all times through which intercepted electronic communications and information relating to the interception will be transmitted to the interception reception centers.[231]
- Intercepted communications must be provided to the interception reception center with a quality no lower than that obtained by the recipient of the communication.

2.2 Access to stored information

Access to stored information is regulated in Sections 2 and 3 of Chapter V CPA. Article 588 ter J, in Section 2, deals with the data contained in automated files of service providers. When knowledge of such data is essential for the investigation, authorization shall be requested from the competent judge to collect the information contained in the automated files of service providers, including cross-referenced or intelligent data searches, provided that the nature of the data to be disclosed and the reasons justifying the transfer are specified.

Chapter V, Section 3 CPA regulates the access to data necessary for the identification of users, terminals, and connectivity devices. When, in the exercise of their duties to prevent and detect crimes committed on the Internet, Judicial Police officers have access to an IP address that is being used to commit a crime and the identification and location of the corresponding computer or connectivity device or the personal identification data of the user are not recorded, they shall request the investigating judge to require the providers of telecommunications to provide the data enabling the identification and location of the terminal or connectivity device and the identification of the suspect (Article 588 ter k). Likewise, when, in the exercise of their duties, the Public Prosecutor's Office or the Judicial Police need to know the ownership of a telephone number or any other means of communication, or, conversely, require the telephone number or identifying details of any means of communication, they may directly contact the providers of telecommunications services, access to a telecommunications network or information society services and these are obliged to comply with the request. A refusal of such a request may result in a penalty for committing the offense of disobedience (Art 588 ter m).

2.3 Active measures

It is noteworthy that the CPA also includes active measures of the interception of telecommunications such as the identification of terminals by capturing identification codes from the device or its components, such as the IMSI or IMEI numbering. (Chapter V, Section 3, Article 588 ter l). Other active measures are included in Chapter VI, which regulates the interception and recording of oral

230 In the case of mobile services, the position of the communication point shall be provided as accurately as possible and, in any event, the identification, location, and type of the base station concerned.

231 The characteristics of these interfaces and the format for the transmission of intercepted communications to these centers will be subject to the technical specifications established by the Ministry of Economic Affairs and Digital Transformation.

communications using electronic devices; Chapter VII, which deals with the registration of mass data storage devices, and Chapter IX which regulates the remote registration of computer equipment.

Although these active measures are undertaken by the police or the secret service and not by the telecommunications provider, some of these measures require the provider's collaboration. That is the case, for example, for the identification of terminals by capturing identification codes from the device or its components (as per Article 588 ter e) and for the remote registration of computer equipment (Article 588 septies b).[232]

2.4 Procedure

Articles 83 to 101 of the Regulation on the Conditions for the Provision of Electronic Communication Services, the Universal Service, and the Protection of Users, approved by Royal Decree 424/2005 of April 15,[233] determine the procedure and measures that service providers and operators of public electronic communication networks must adopt to intercept communications when required by law. That Regulation establishes the general requirements of the procedure, access requirements, and the information to be delivered to the authorized agent (judicial police or CNI agent), as well as other operational requirements, such as previous information, locations, authorized personnel, confidentiality, real-time access, and interception interfaces.[234]

Additionally, Article 58 of Law 11/2022 sets out the operator's duty to intercept communications when required by the relevant authorities. This should be done through the appropriate interfaces and technical resources, which should be ready for this purpose.

3. How does the law in Spain regulate data retention?

The storage and transfer of data generated or processed in the course of providing electronic communications services or public communications networks to authorized agents through the corresponding judicial authorization for the purposes of detecting, investigation, and prosecution of serious crimes covered by the Criminal Code or special criminal laws is mainly governed by the provisions of Law 25/2007, of October 18, on the retention of data relating to electronic communications and public communications networks,[235] although the Spanish Criminal Procedure Act (CPA) also includes data retention provisions.

---

232 Under Article 588 septies b CPA, service providers and the owners or persons responsible for the computer system or database subject to registration are required to provide investigating officers with the necessary cooperation to carry out the measure and access the system. They are also required to provide the necessary assistance so that the data and information collected can be examined and viewed. The authorities and agents in charge of the investigation may order any person who is familiar with the operation of the computer system or the measures applied to protect the computer data contained therein to provide the information necessary for the proper conduct of the proceedings. Persons required to cooperate shall be obliged to maintain secrecy regarding the activities requested by the authorities.

233 Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, available at: https://www.boe.es/eli/es/rd/2005/04/15/424/con (02.07.2025).

234 CLFR, op. cit.

235 Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, https://www.boe.es/eli/es/l/2007/10/18/25/con

3.1 Law 25/2007

Law 25/2007 transposed the 2006 EU Data Retention Directive (Directive 2006/24/EC of the European Parliament and of the Council of March 15) into Spanish law. Unlike other Member States that chose to include the content of the Directive in other laws, such as those relating to telecommunications, Spain did so by means of a specific law.[236]

Law 25/2007 applies to traffic and location data relating to natural and legal persons and to the related data necessary to identify the subscriber or registered user. The obligations relating to data retention and transfer imposed by that Law apply only to operators providing publicly available electronic communications services or operating public communications networks.[237]

Such duties to hold and provide information are not precisely the same as those of the SPTA, and some provisions are not included, like those referring to the information to identify perpetrators of criminal offences via the internet and to identify persons in the case of threats to internal or external security (Art. 22 SPTA). Most importantly, the content of electronic communications, including information accessed using an electronic communications network, is excluded.[238]

It is important to note that the Law 25/2007 also imposes a requirement of "prior judicial authorization" to transfer the data, which was not included in the 2006 Directive.

Article 3 of Law 25/2007 provides a precise and detailed list of the data subject to retention requirements in the context of fixed, mobile, and Internet communications.[239]

The data subject to retention (those that will not be deleted or anonymized and must be stored or retained) includes:

- data necessary to trace and identify the origin of a communication (calling telephone number, name and address of the user, IP identification, etc.)
- data necessary to identify the destination of a communication (number or numbers dialed, names and addresses of users, user identification, IP identification, recipient user identification)
- data necessary to identify the date, time, and duration of a communication (date and time of the beginning and end of the communication, date and time of connection and disconnection from the Internet access service, date and time of connection and disconnection from the email service, etc.)
- data necessary to identify the type of communication (telephone service used, Internet service used)
- data necessary to identify users' communication equipment or what is considered to be communication equipment (source and destination telephone numbers, source IMSI, source IMEI, recipient IMSI, recipient IMEI, digital subscriber line (DSL), communication author's terminal point identifier, etc.)

---

236 Andoni Polo Roca, La conservación de datos en el sector de las telecomunicaciones. Un estudio sobre su regulación en la Unión Europea y su cabida en el Derecho de la Unión Editorial Aranzadi, S.A.U., 1.ª Ed., 2022.

237 Ley 25/2007, Art. 2.

238 Ley 25/2007, Art. 1.

239 In accordance with the provisions of the EU Data Retention Directive, unsuccessful telephone calls are also within the scope of the law. This includes the obligation to retain sufficient information to identify when prepaid phones are activated.

- data necessary to identify the location of mobile communication equipment (location tag, geographical location)

The data that must be retained includes both natural and legal persons. However, in no case is the provider to reveal the content of the communication. The container is therefore retained, but under no circumstances the content.

It is important to note that in a ruling of 8 April 2014 ("Digital Rights Ireland"), the Court of Justice of European Union (CJEU) annulled the EU Data Retention Directive.[240] However, even though the EU Data Retention Directive serves as the basis for the Law 25/2007, the latter law has not been repealed. The potential contradiction between Law 25/2007 and the CJEU decisions to invalidate the EU Data Retention Directive has been addressed by the Spanish Supreme Court (Tribunal Supremo), in a judgment upholding the validity of Law 25/2007. The decision analyzes EU law, the most important rulings of the CJEU, and the provisions of Law 25/2007, concluding that Law 25/2007, taken as a whole, is not contrary to EU law. It also states that, even if Law 25/2007 may be deficient in some respects, in order to establish that the right recognized in Article 18.3 of the Spanish Constitution has been infringed[241], it is necessary to determine in each case whether the interference was based on evidence of criminality, was necessary and proportionate, and complied with the other requirements of any limitation of fundamental rights.[242]

3.2 Spanish Criminal Procedure Act

The CPA also includes a general provision on data retention (Article 588 octies)

> Article 588 octies. Data retention order.
>
> The Public Prosecutor's Office or the Judicial Police may require any natural or legal person to retain and protect specific data or information contained in a computer storage system at their disposal until the relevant judicial authorization for its transfer is obtained in accordance with the provisions of the preceding articles.
>
> The data shall be retained for a maximum period of ninety days, which may be extended once until the transfer is authorized or one hundred and eighty days have elapsed.
>
> The person requested shall be obliged to cooperate and to maintain secrecy regarding the conduct of this procedure, and shall be subject to the liability described in section 3 of Article 588 ter e.

---

240 The CJEU considered that the directive "entails a wide-ranging and particularly serious interference with the fundamental rights to the respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary". CJEU, Judgment of the Court (Grand Chamber), 8 April 2014. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, available at : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0293 (02.07.2025).

241 Article 18.3 of the Spanish Constitution guarantees the secrecy of communications, especially postal, telegraphic, and telephone communications, except by court order.

242 In the case at hand, the transfer of the stored data was justified, necessary, proportionate, and aimed at investigating serious crimes (robbery with violence and three illegal arrests). Furthermore, in this specific case, the transfer of the data collected by the judge was legal because it was supported not only by Law 25/2007 but also by the Telecommunications Law, which allowed storage for commercial and billing purposes. Sentencia Penal Nº 727/2020, Tribunal Supremo, Sala de lo Penal, Sección 1, Rec 4218/2018 de 23 de Marzo de 2021, available at: https://www.iberley.es/jurisprudencia/sentencia-penal-n-727-2020-ts-sala-penal-sec-1-rec-4218-2018-23-03-2021-48350124 (02.07.2025)

This data preservation order is also called “quick freeze”, and it was introduced by the Budapest Convention on Cybercrime of the Council of Europe,[243] specifically in Articles, 16, 17, 29, 35 (“Expedited preservation”).

4. How does the Spanish law regulate the retention of boundary data (“Randdaten”)?

The data subject to retention according to Law 25/2007 includes the data used for the technical transmission of messages, or “boundary data” (e.g. the addressing data in the header of electronic messages and information on the connection setup according to the technical communication protocol).

According to that law, the data to be retained consists of all data relating necessary to trace and identify the origin and destination of a communication (telephone numbers, name and address of the users, IP identification, etc.), the data necessary to identify the date, time, and duration of a communication, the data necessary to identify the type of communication (telephone or Internet service used), the data necessary to identify users' communication equipment (telephone numbers, IMSI, IMEI, DSL, communication author's terminal point identifier, etc.), and the data necessary to identify the location of mobile communication equipment (location tag, geographical location).

5. How long must providers in Spain retain data?

Article 5 of Law 25/2007 establishes the data retention period as generally twelve months from the date on which the communication was established. This may be reduced to six months or extended to two years, as permitted by Directive 2006/24/EC.[244]

In addition, specific provisions are established with regard to the general regime governing the rights of access, rectification, and cancellation of data contained in the aforementioned Organic Law 15/1999.

The stored data may only be transferred with prior judicial authorization for the purposes of detecting, investigation, and prosecution of serious crimes covered by the Criminal Code or special criminal laws. The transfer of information shall be carried out in electronic format only to authorized agents[245] and shall be limited to the information that is essential for the achievement of the purposes of detecting, investigation, and prosecution of serious crimes.

---

243 Budapest Convention on Cybercrime of the Council of Europe, ETS No. 185, available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention (02.07.2025).

244 Article 5 also sets out the instruments to ensure the legitimate use of the data retained, which may only be transferred and delivered to the authorized agent and for the purposes established in the Law, any misuse being subject to the control mechanisms of Organic Law 15/1999, of December 13, on the Protection of Personal Data and its implementing legislation (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, available at: https://www.boe.es/eli/es/lo/1999/12/13/15/con (02.07.2025)).

245 For these purposes, the following are considered authorized agents: a) Members of the security forces and bodies, when performing judicial police functions, b) Officials of the Deputy Directorate of Customs Surveillance, in the exercise of their powers as judicial police, c) The staff of the National Intelligence Center in the course of security investigations on individuals or entities.

6. Rules regarding un-encrypting

In Spain, service providers are generally not required to decrypt their users' communications or data. However, if in case of interception of telephone or telematic communications they have applied any compression, encryption, digitization, or any other type of coding to the communications subject to lawful interception, service providers must deliver those communications to the authorities without the effects of such procedures (e.g. un-encypted), provided that they are reversible.[246]

246 Art. 58.11 Law 11/2022.

G. SWEDEN

Introduction and legal basis

The main pieces of legislation and Government ordinances regulating electronic communication, including obligations of providers of telecommunication and communication services, are:

Legislation:

- Lag (2022:482) om elektronisk kommunikation (Electronic Communication Act - ECA, available in Swedish at https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2022482-om-elektronisk-kommunikation_sfs-2022-482/
- Lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (Electronic Intelligence Act), available in Swedish at Lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet | Sveriges riksdag
- Rättegångsbalk (1942:740) (Code of Judicial Procedure), available in Swedish at https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/rattegangsbalk-1942740_sfs-1942-740/

Government ordinance:

- Förordning (2022:511) om elektronisk kommunikation (Government Ordinance on Electronic Communication (OEC), available in Swedish at Förordning (2022:511) om elektronisk kommunikation | Sveriges riksdag

EU law

The Swedish legal instruments implement the requirements in a number of EU law instruments, in particular:

- Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
- (Repealed) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

Study on Data retention law in the Nordic countries

The Nordic council conducted a recent study in English on data retention law in the Nordic countries. This study, available at https://pub.norden.org/temanord2024-532/temanord2024-532.pdf, provides detailed information, inter alia, on the obligations of service providers to retain data and obligation to disclose data to law enforcement authorities.

Supervisory authority

The Swedish Post and Telecom Authority (*Post- och telestyrelsen - PTS*) is the regulatory authority and supervisory authority under the Electronic Communications Act. Other authorities, such as the Swedish Economic Crime Authority, the Swedish Police Authority, the Swedish Security Service and the Swedish Prosecution Authority also play a role, often as authorities that must be consulted by the PTS before it issues regulations.

The PTS does not itself retain data from providers of telecommunication services. Obligation duties to retain data apply to the providers of telecommunication services.

1. Does Sweden have different categories of telecommunication providers that are similar to those of the telecommunication service providers (*Anbieter von Fernmeldediensten, FDA*) and providers of derived communications services (*Anbieter von abgeleiteten Kommunikationsdiensten, AAKD*) in Swiss law?

Swedish legislation **distinguishes between providers of telecommunication services and providers of number-independent interpersonal communications, so-called NI-ICS services**. This follows the logic in the Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

For the purpose of retention obligations based on law enforcement considerations, the Swedish Electronic Communication Act (ECA) lays down general obligations that apply only to providers of telecommunication services (Chapter 9 section 19).

The Government-appointed Law Commission *SOU 2023:22 Datalagring och åtkomst till elektronisk information* (Data retention and access to electronic information) has in its report proposed amendments to the Swedish law.[247] An **important proposition in the Law Commission's report is to include Providers of so-called NI-ICS services (such as e Apple iMessage, Apple FaceTime, Discord, Snapchat, Google Messages, and Whatsapp, etc.) to be bound by the obligation of retention applicable to providers of telecommunication services**. This proposal has been incorporated into the Government's draft bill, which is **scheduled to enter into force on 1 March 2026.**[248]

2. What surveillance and information obligations do telecommunication service providers have in Sweden?

Providers must enable lawful surveillance of electronic communications and give access to retained data if the competent authority decides to request it. This is regulated in the Electronic Intelligence Act (*Lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*) and in the Code of Judicial Procedure (*Rättegångsbalk (1942:740)*). The **access concerns all retained data that must be stored**. The type of

---

247 The report is available in Swedish, including a summary in English, at https://www.regeringen.se/contentassets/35276188514d40fb87785c81c0fbda93/datalagring-och-atkomst-till-elektronisk-information-sou-202322/) (18.06.2025).

248 Utkast till lagrådsremiss Datalagring och tillgång till elektronisk information p. 86, available at https://www.regeringen.se/rattsliga-dokument/departementsserien-och-promemorior/2024/11/utkast-till-lagradsremiss-datalagring-och-tillgang-till-elektronisk-information/ (22.09.2025).

data that must be stored is described below (see question 3) and includes, as regards internet access, users IP-addresses and other **data necessary to identify a subscriber and registered user**.[249] It should be noted that the **storage obligation does not extend to providers of number-independent interpersonal communications**, so-called NI-ICS services (such as Apple iMessage, Apple FaceTime, and WhatsApp). However (and as mentioned above), there is a draft bill proposing that such providers should be subject to the same retention obligations as telecommunication service providers.

According to Chapter 27 section 19 of the Code of Judicial Procedure, **data can be disclosed to the police in the investigation of an offence** (including attempt and preparatory acts) punishable with imprisonment for a minimum period of 6 months or more, as well as for a number of specifically listed offences (including hacking, child pornography offences, drug offences). Generally, the courts decide on the disclosure of information upon request by the prosecutor.[250]

The **Electronic Intelligence Act** provides for the collection of data when considered necessary for **intelligence activities aimed at preventing, intervening against, or uncovering criminal activities** as further specified in that act. The targeted criminal activity must involve an offence with a prescribed penalty of imprisonment for at least 2 years or other offences as specified in the act. The prosecutor decides on the collection of data for intelligence purposes upon request by either the Police Authority, the Police Security Service or the Customs Authority.[251]

3. How does the law in Sweden regulate data retention?

Data retention is primarily regulated in the ECA. Chapter 9 section 19 of the ECA provides that the **obligation to register and store data** for the purpose of law enforcement comprises anyone who conducts activities that must be notified to the Post and Telecom Authority. This notification requirement concerns **anyone who offers a service of "public communications networks that are usually provided against compensation or publicly available electronic communications services"**.[252] Providers of number-independent interpersonal communications, so-called **NI-ICS services, are excluded from this obligation** (however, there is a **proposal** from a government appointed law committee **to include these providers also**; *see above reply to the first question*).

The **data to be registered and stored are broadly specified in Chapter 9 section 19 of the ECA**, supplemented by the more detailed regulation in the Government Ordinance on Electronic Communication (*Förordning (2022:511) om elektronisk kommunikation*) chapter 9 section 7 and 8. It **comprises all data necessary to trace and identify** the **source** of the communication, the final **destination** of the communication, **date, time, and duration** of the communication, **type** of communication, communication **equipment**, as well as the **location** of mobile communication devices at the time of the communications' beginning and end.[253] This includes data about the **subscription**. (For further information in English, see the Study on data retention law in the Nordic countries, p. 65 ff.)

---

249 Förordning (2022:511) om elektronisk kommunikation (Government Ordinance on Electronic Communication (OEC), Chapter 9 section 8. See also The Nordic Council's study Data Retention Law in the Nordic Countries, p, 66 ff, available at https://pub.norden.org/temanord2024-532/temanord2024-532.pdf (18.06.2025).

250 Code of Judicial Procedure Chapter 27 section1.

251 Electronic Intelligence Act section 3.

252 ECA Chapter 2 section 1.

253 ECA Chapter 9 section 19.

The **access to the retained data for law enforcement purposes** is regulated in the ECA, in the Electronic Intelligence Act (*Lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*), and in the Code of Judicial Procedure (*Rättegångsbalk (1942:740*)).[254]

4. How does the law regulate the retention of boundary date ("Randdaten")?

There is no data referred to as "boundary data" in the Swedish legislation. As mentioned in the previous question, the data to be retained is specified in Chapter 9 section 19 of the ECA. Essentially it includes all data necessary to trace and identify the source of the communication, the final destination of the communication, date, time, and duration of the communication, type of communication, communication equipment, as well as the location of mobile communication devices at the time of the communications' beginning and end.

The relatively general wording in the Swedish regulation is intended to make it more resilient to changes caused by technical development. It encompasses the data that are relevant for the stated purpose under any given technical solution (see more on the data to be retained in the Study on data retention law in the Nordic countries, p. 65 ff.).

5. How long must providers in Sweden retain data?

The **retention period depends on the type of information, ranging from two months to ten months** after the communication ended. The storage obligation of providers of telecommunication services is regulated in Chapter 9 of the ECA. Chapter 9, Section 22 provides that "information referred to in Chapter 9 section 19 shall be stored as follows:

- Information generated or processed in connection with telephone services and message handling via mobile network access points must be stored for **six months.** However, location data must be stored for only **two months.**
- Information generated or processed in connection with Internet access must be stored for **ten months**. However, if the data identifies the equipment where the communication is finally secluded from the storage provider to the subscriber, it must be stored for only six months.
- The **storage period is calculated from the date on which the communication ended**. When the storage period has expired, the storage **provider must immediately erase** the data.

6. Rules regarding the removal of encryption

The legal situation as regards access of law enforcement authorities to encrypted information is rather complex. There is currently **no explicit legal obligation requiring telecommunication service providers or other actors to remove encryption from their services or communications**. However, telecommunication service providers have a far-reaching obligation to assist law enforcement authorities in accessing the information requested (including encrypted information) to the extent this is technically possible for the service provider. In many cases the telecommunication service providers are not able to remove the encryption, typically when the encryption is embedded in a communication service/product of a third party.

254 ECA Chapter 9 section 21.

As mentioned above, a **2024 draft bill proposes legislation requiring all communication service providers (including providers of so-called NI-ICS services) to adapt their Services/products (*anpassingsskyldighet*) so that they can provide the information requested by law enforcement agencies**.[255] While the draft bill does not contain any explicit obligation to remove encryption, the proposed legislation requires that it must be technically possible to receive the information requested in a readable format.[256] This implies that service providers (including NI-ICS services) must adapt their product so that it is possible to provide encrypted information in a readable format.

The **draft bill has been subject to criticism** by some stakeholders arguing that this cannot be achieved without the use of so-called encryption backdoors, which they argue would be a risk to secure communications.[257] It should also be noted that it has not yet been submitted to the Council on Legislation (*Lagrådet*), which examines if the draft bill is compatible with the constitution and general legal principles. The legislation is scheduled to enter into force on 1 March 2026.[258]

---

255 Utkast till lagrådsremiss Datalagring och tillgång till elektronisk information, available at https://www.regeringen.se/rattsliga-dokument/departementsserien-och-promemorior/2024/11/utkast-till-lagradsremiss-datalagring-och-tillgang-till-elektronisk-information/ (22.09.2025).

256 Ibid.

257 See for instance https://www.statewatch.org/news/2025/april/swedish-parliament-urged-to-reject-law-that-would-greatly-undermine-security-and-privacy/#:~:text=The%20legislation%20would%20force%20companies,every%20door%20in%20a%20building (22.09.2025).

258 Utkast till lagrådsremiss Datalagring och tillgång till elektronisk information, available at https://www.regeringen.se/rattsliga-dokument/departementsserien-och-promemorior/2024/11/utkast-till-lagradsremiss-datalagring-och-tillgang-till-elektronisk-information/ (22.09.2025).

H. UNITED KINGDOM

Overview

In the UK, the main law concerning the scope and definitions of telecommunications activity, access to and, the retention of, communications data is the Investigatory Powers Act 2016 **('IPA 2016').** This provides the principal framework governing the powers of UK public bodies, including intelligence and security agencies and police enforcement, to intercept, acquire, or seek the retention of, communications data.[259] Parts of the IPA 2016 were recently amended by the Investigatory Powers (Amendment) Act 2024 **('IP(A)A 2024')**, widening the scope of the government's access to certain electronic datasets. This is discussed below.

More recent legislation, the Telecommunications (Security) Act 2021 **('T(S)A 2021')**, does not concern telecommunications surveillance or access to telecommunications data, but rather establishes a cybersecurity framework. Together with the Electronic Communications (Security Measures) Regulations 2022, it sets out a wide range of security duties on what are termed providers of 'public electronic communications networks' (see below). It focuses on strengthening the security of telecommunications networks and services, primarily by requiring providers to implement security measures and manage their supply chains effectively.

1. Does the UK have different categories of telecommunication providers that are similar to those of the telecommunication service providers (Anbieter von Fernmeldediensten, FDA) and providers of derived communications services (Anbieter von abgeleiteten Kommunikationsdiensten, AAKD) in Swiss law?

In both the IPA 2016 and the T(S)A 2021, the target of the legal provisions – in the IPA 2016, '*telecommunications operators'* and in the T(S)A 2021, '*providers of public electronic communications networks/services*' – are defined broadly, and there is **no distinction made between internet service providers and what might be termed 'derived communication service providers',** such as web-based email services and instant messaging applications.

1.1 The IPA 2016

The IPA 2016 refers to 'telecommunications operators'. A **UK Government Code of Practice** (the *Communications data code of practice*) has been issued to provide technical guidance to those subject to the IPA 2016. It was **updated in June 2025**, in part, to reflect changes introduced by the IP(A)A 2024. It states that a '**telecommunications operator'** is,

> "a person who offers or provides a telecommunications service to persons in the UK; controls or provides a telecommunication system which is (wholly or partly) in or controlled from the UK; or controls or provides a telecommunication system which is not (wholly or partly) in, or controlled from, the UK and is used by another person to offer or provide a telecommunications service to persons in the UK ."[260]

---

259 It also adopts certain provisions previously contained, and now repealed, in the *Data Retention and Investigatory Powers Act 2014.*

260 *Communications data code of practice*, para. 2.1.

The IPA 2016 defines '**telecommunications service'** to mean any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service);[261] 'telecommunication system' is defined as:

> "[…] any system (including the apparatus comprised in it) that exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy."[262]

The **definitions of 'telecommunications service' and 'telecommunication system' in the IPA 2016 are said to be intentionally broad** so that they remain relevant for new technologies.[263]

The Code of Practice states that the IPA 2016:

> "makes clear that any service which consists in, or includes, facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of a telecommunication system is included within the meaning of 'telecommunications service'. **Internet based services such as web- based email, messaging applications and cloud-based services are covered by this definition**."[264]

The newly updated version of the **Code of Practice includes a non-exhaustive list of examples of telecommunications operators**.[265] These include any website owner. This is because the provision of the website is said to constitute a telecommunications service by itself, regardless of whether it includes a chat function. The list includes the following:

- providers of public telephony services
- Internet service providers
- the provider of any app that interfaces with the Internet
- Webmail providers
- online marketplaces
- streaming platforms
- social media platforms
- online dating sites
- online gaming companies and platforms
- online betting and casinos
- taxi companies (a taxi company with no online presence is not a Telecommunications Operator as defined in the Act)
- providers of telecommunications services to SIMs embedded in vehicles
- food delivery services
- video conferencing and VoIP providers (voice-over internet protocol)
- Cloud providers
- instant messaging apps
- banks with an online presence and digital banking system
- online payment processors

---

261 *IPA 2016, op. cit.,* s. 261(11).

262 *Ibid*, section 261(13).

263 *Communications Data Code of Practice*, *op. cit.,* para. 2.7.

264 *Ibid,* para. 2.6.

265 *Ibid,* para. 2.8.

- top up services

1.2. The T(S)A 2021

Adopting the definition used in the Communications Act 2003 (the 2003 Act), **the T(S)A 2021** applies to **'providers of public electronic communications networks'** and **'providers of public electronic communications services'**.

Section 151 of the **2003 Act defines** both of these terms. A '**public electronic communications network'** is: "*an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to the public*." A '**public electronic communications service**' means "*any electronic communications service that is provided so as to be available for use by members of the public*". The 'communications network' definition refers to any transmitter or transmission system (plus associated equipment, software and stored data) used to convey electronic signals (including sounds, images or data of any description). The 'communications service' definition refers to any service that members of the public can sign up to in order to send or receive electronic signals (including sounds, images or data of any description).[266]

These definitions are interpreted very widely to include almost all forms of electronic communication used by the public. They are considered to include internet and mobile phone networks available to the public and it has been ruled to include social media platforms which operate via the internet such as WhatsApp.[267]

We have found no clear explanation of the difference between a 'telecommunications operator', used by the IPA 2016, and an electronic communications network or service referred to in the **T(S)A 2021**. The latter, however, **specifically requires that the network or service is public and has members of the public as customers**, rather than constituting a private or restricted network or service.

It should be noted that the security measures set out in the **2022 Regulations do not apply to what are termed 'micro-entities'**. These are defined as a registered body that satisfies two of the following criteria within the most recent financial years: turnover of not more than £632,000; balance sheet total of not more than £316,000; and a total number of employees of not more than 10.

2. What surveillance and information obligations do telecommunication service providers have in the UK?

2.1. The IPA 2016

Telecommunications operators can be compelled under the IPA 2016 to provide for the **interception** of communications of their users and the **acquisition** of communications data to enable access by police, security agencies and other related public bodies. They can also be placed under a duty to facilitate the **lawful interference** by police, intelligence services and others with **telecommunications**

---

266 See Information Commissioner's Office, *Key concepts and definitions,* last updated 21st August 2023, available at https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/key-concepts-and-definitions/#publicservice (22.05.2025).

267 See *DPP v. Bussetti* [2021] EWHC 2140 (Admin).

equipment. As explained further below,[268] they can also be required to **retain telecommunications data**.

Duty to provide for the interception of telecommunications

The IPA 2016 reformed the regime under which UK law enforcement bodies and intelligence agencies can be authorised by warrant to **intercept and examine communications**.[269] Such a warrant will only be issued where it is necessary, proportionate and justified in the interests of – among other things - national security, the economic wellbeing of the UK, or in support of the prevention or detection of serious crime.[270] **Telecommunications operators have a duty to take all steps for giving effect to the warrant**, and a failure to do so is a criminal offence.[271]

2.1.1. Duty to provide for the acquisition of telecommunications data

UK law also provides for a **duty to be placed on telecommunications operators to obtain or disclose communications data** in response to an authorised request for that data. This is referred to by the IPA 2016 as the **acquisition of communications data** (that is, metadata - the '**who', 'where', 'when', 'how' and 'with whom' of a communication**, but not what was written or said).

This can therefore mean that all telecommunications operators, including encrypted email services and encrypted instant messaging apps such as WhatsApp, can be **compelled to disclose information which can identify an individual**, such as sender and recipient details, user account information, IP addresses and device details, even if those operators are technically unable to access the content of end-to-end encrypted messages.

It is recognised under UK law that the acquisition of communications data will be a justifiable interference with an individual's human rights only if the conduct being authorised or required to take place is necessary for the purposes of a specific investigation or operation, proportionate and in accordance with law. The **duty of a telecommunications operator to respond to such a request** only arises on that operator being issued with a notice requiring them to do so.[272] There is therefore **no blanket or ongoing general requirement on any telecommunications providers** to allow access or to disclose communications data.

Before public authorities, including the police and the security and intelligence agencies, can acquire targeted communications data, **authorisation must be given by the relevant individual.**[273] An

---

268 In sections 3, 4, and 5 of this country report.

269 The interception of communications can (save in other prescribed circumstances, such as with the consent of the sender and recipient) only lawfully be undertaken pursuant to a warrant issued by the Secretary of State (the relevant government minister) and must be approved by Judicial Commissioner (namely, an independent judge). Before an interception warrant can be issued, the Secretary of State must believe that a warrant is necessary on certain, limited grounds, and that the interception is proportionate to what it seeks to achieve. These grounds are that interception is necessary:
- In the interests of national security; or
- In the interests of the economic well-being of the UK; or
- In support of the prevention or detection of serious crime

The IPA 2016 also requires safeguards to be in place to limit the use of intercepted material and related communications data.

270 IPA 2016, Part 2.

271 IPA 2016, section 43.

272 IPA 2016, section 66.

273 Namely – depending on the case - a public official known as the Investigatory Powers Commissioner or the designated senior officers of the relevant public authority.

application for that authorisation must include an explanation of **why it is necessary for one or more statutory purposes set out in the IPA 2016** (these include national security, for an applicable crime purposes, in the interests of public safety etc).[274] Access to internet connection records is subject to additional restrictions.[275] The duty on the telecommunications operator to comply with a requirement to obtain or disclose communications data is enforceable by civil proceedings brought by the Secretary of State (the relevant government minister).[276]

2.1.2. Duty to facilitate interference with equipment

A further **duty on telecommunications operators** may arise where they are served with notice of a warrant, obtained by law enforcement officers, intelligence services or the Chief of Defence Intelligence **to interfere with equipment for the purpose of obtaining communications or equipment data**.[277] Telecommunications operators are required to take all steps for giving effect to the warrant, and this duty is enforceable by civil proceedings by the Secretary of State for an injunction, specific performance or any other appropriate relief.[278]

2.1.3. Duty to facilitate bulk interception/acquisition

The IPA 2016 also provides for a duty to be placed on a telecommunications operator pursuant to a warrant for what is known as the **bulk interception or acquisition of communications data (and bulk interference with equipment)**. This is where there is no limit on the volume of communications data which may be acquired. It is an intelligence gathering capability rather than – as in the case of a targeted communications data interception or acquisition - an investigative tool used to intercept or acquire data in relation to specific investigations. Like a targeted communications data interception or acquisition, this requires a warrant to be served on a telecommunications operator, but a bulk interception or acquisition warrant may only be sought by an intelligence service[279] and the warrant can only be granted by the relevant government minister, the Secretary of State, and approved by an independent judge, known as a Judicial Commissioner. A warrant will only be granted where it is considered necessary and proportionate to do so for the purposes of the intelligence service's statutory functions, including the protection of national security. **Telecommunications operators are under a specific duty to take all steps for giving effect to a bulk acquisition warrant**.[280]

2.1.4. Duty to notify of planned changes

It should also be noted that the IP(A)A 2024 has introduced a new power for the Secretary of State to **require telecommunications operators to notify the government in advance of any planned changes to its services or their functionality**.[281] The aim of this requirement is to prevent technological changes – such as the introduction of end-to-end encryption – from having a detrimental effect on the powers and capabilities of the police and intelligence services.[282] This could include preventing them from

---

274 IPA 2016, section 60A(7) and corresponding subsections for other individuals capable of granting authorisations.

275 IPA 2016, section 62.

276 IPA 2016, section 66(5).

277 IPA 2016, Part 5.

278 IPA 2016, section 128(7).

279 *Ibid*, section 158.

280 IPA 2016, section 170(1).

281 IPA 2016, section 258A(1), as introduced by the IP(A)A 2024, section 21.

282 DLA Piper, *UK: Changes to UK surveillance and communications law: the Investigatory Powers (Amendment) Act 2024*, available at https://www.gov.uk/government/publications/investigatory-powers-amendment-bill-factsheets/investigatory-powers-amendment-bill-notification-

accessing the capabilities and communications related data needed to prevent crime and protect national security. The requirement of notification is concerned with changes that will affect the police and intelligence services when lawfully accessing data where such a consequence can be *"reasonably anticipated by the operator, even if this is not the primary motivation."*[283]

2.2. The T(S)A 2021

The T(S)A 2021 amended the UK's principal communications law, the Communications Act 2003, by requiring telecommunications providers to have measures in place to identify and defend their networks from cyber threats, as well as to prepare for any future risks. The Act also introduces **new national security powers** for the Government to impose, monitor and enforce controls on public communications providers' use of designated vendors' goods, services and facilities within UK telecommunications networks. There are no specific surveillance and information obligations contained in the T(S)A 2021. These are rather reserved to the IPA 2016.

The **framework established through the T(S)A 2021 comprises three layers**: (1) overarching security duties on public telecommunications providers; (2) specific security measures set out in secondary legislation – the *Electronic Communications (Security Measures) Regulations 2022* ('the 2022 Regulations'), setting out the specific security measures that public telecom providers must implement; (3) a code of practice detailing guidelines to large and medium-sized providers of public telecommunications providers (see definitions below) on the government's preferred approach to demonstrating compliance with the duties in the Act.

Some of the more significant **duties set out in the 2022 Regulations** include:

- A duty to protect network architecture i.e. by securely designing and constructing (or redesigning and developing in instances of existing network architecture) public networks to reduce risks of security compromises, as well as keeping a record of the risks identified;
- A duty to protect tools enabling monitoring and analysis from high-risk and hostile state actors;
- A duty to monitor and analyse access and changes to the networks or service by retaining records / logs for at least 13 months;
- A duty to deploy patches or mitigations, and upgrade and implement security updates within an appropriate period;
- A duty to carry out testing at appropriate intervals to identify risks of security comprises; and
- A duty to share information with other providers and help remedy or mitigate the effects of any security issues, but only for the purposes of identifying and reducing security risks.

The Regulations require network and service providers to **take responsibility for supply chain risks**. This includes having appropriate and proportionate contractual arrangements in place requiring third party suppliers to identify, disclose and reduce risks of security compromises arising from the relationship. Providers must also ensure written contingency plans are in place in the event that supply from third party is interrupted.

---

requirement#what-happens-when-a-notification-requirement-is-submitted-by-a-telecommunications-operator (08.07.2025).

283 Home Office, *Policy paper – Investigatory Powers (Amendment) Bill: Notification Requirement*, updated 26th April 2024, available at https://www.gov.uk/government/publications/investigatory-powers-amendment-bill-factsheets/investigatory-powers-amendment-bill-notification-requirement#what-happens-when-a-notification-requirement-is-submitted-by-a-telecommunications-operator (08.07.2025).

Network or service providers are also required to take appropriate and proportionate measures **to ensure those given responsibility for securing the networks are managed appropriately and are adopting suitable security measures**. Providers must assign someone of board-level to oversee any new governance processes and ensure the management of those with responsibility for securing the network.

3. How does the law in the UK regulate data retention?

No telecommunications operator is required to retain any data under the IPA 2016 until given a notice to do so (known as a "*retention notice*").

The IPA 2016 provides that communications service providers may be required by such a notice issued by the Secretary of State to **retain communications data**.[284] A retention notice may only be issued for specific statutory purposes,[285] where it is considered necessary and proportionate to do so and where that decision has also been approved by a Judicial Commissioner.[286] The specific statutory purposes are as follows:

(i) in the interests of national security;

(ii) for the purpose of preventing or detecting serious crime or for preventing or detecting crime or of preventing disorder;

(iii) in the interests of the economic well-being of the UK so far as those interests are also relevant to national security;

(iv) in the interests of public safety;

(v) for the purpose of preventing death/injury or any damage to a person's physical/mental health or of mitigating any injury/damage to a person's physical or mental health;

(vi) to assist investigations into alleged miscarriages of justice.

There is no known publicly available information with regard to statistics concerning the issue of data retention notices.

4. How does the law regulate the retention of boundary date ("Randdaten")?

The only communications data that may be retained by telecommunications operators under UK law is **that specified in a retention notice** issued by the Secretary of State pursuant to the IPA 2016 (see response to question 3, above). This is specifically identified in the IPA 2016 as "***relevant communications data***", and its statutory definition most closely corresponds to the type of data understood to constitute *Randdaten*.[287] Relevant communications data is described in the IPA 2016 as meaning communications data which may be used to identify or assist in identifying any of the following:

---

284 IPA 2016, section 87(1).

285 IPA 2016, section 87(2). These are set out in the main text, below.

286 IPA 2016, section 87(1).

287 IPA 2016, section 87(11).

(i) the sender or recipient of a communication (whether or not a person),

(ii) the time or duration of a communication,

(iii) the type, method or pattern, or fact, of communication,

(iv) the telecommunication system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted, or

(v) the location of any such system,

The Act states that such data includes, in particular, internet connection records.

5. How long must providers in the UK retain data?

A retention notice must not require any data to be retained for more than **12 months**.[288] An amendment to the IPA 2016, introduced by the IP(A)A 2024, means, however, that a retention notice can be renewed for up to a further 12-month period by the Secretary of State in the 30-day period prior to the expiry of the original notice. This is subject to approval by a Judicial Commissioner.[289]

6. Rules regarding the removal of encryption

Under the IPA 2016, the Secretary of State (the relevant government minister) may, on behalf of the UK Government, **issue a relevant telecommunications operator** with **a 'technical capability notice' ('TCN')[290] requiring it to remove electronic protection on communications or data** on an ongoing basis.[291] A TCN compels a telecommunications operator to develop and maintain the technical abilities needed to assist with law enforcement and intelligence agency investigations. For encrypted services, this can include **un-encryption capabilities in order to allow the creation of what is referred to as a 'backdoor' into secure communications channels**. A TCN must be proportionate to what is sought to be achieved and is also subject to approval by a Judicial Commissioner.[292] The existence and contents of the notice cannot be disclosed[293] and it can, moreover, be issued to companies outside the UK, potentially requiring actions to be taken overseas.[294]

However, a **telecommunications operator cannot be required to take any steps which it is not reasonably practicable** for them to take.[295] What is reasonably practicable will be considered on a case-by-case basis, taking into account the **individual circumstances of the relevant telecommunications operator**.[296] One of the five sets of obligations identified by the IPA 2016 that may be specified by the Secretary of State are obligations which relate to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications data.[297] Section 255(4) of the IPA 2016 states in relation to electronic protection, such as encryption:

---

288 IPA 2016, section 87(3).

289 IPA 2016, section 94A.

290 IPA 2016, section 253.

291 IPA 2016, section 253(7).

292 IPA 2016, section 253(1).

293 IPA 2016, section 255(8).

294 IPA 2016, section 253(8).

295 IPA 2016, section 253(4).

296 *Communications data code of practice, op. cit.,* at para. 14.2.

297 IPA 2016, section 253(5)(c).

> "In the case of a technical capability notice that would impose any obligations relating to the removal by a person of electronic protection applied by or on behalf of that person to any communications or data […], the Secretary of State must in particular take into account the **technical feasibility, and likely cost, of complying with those obligations**."

Telecommunications operators, such as WhatsApp, who provide end-to-end encrypted communication services, state that their encryption protocol means that only the user and the recipient of communications can listen to or read what is being sent, and that it – as the telecommunications operator – is technically unable to access the content of those communications.[298] Such **telecommunications operators, for whom it is not technically feasible to provide access to encrypted communications**, claim that it is not possible for them to comply with a TCN which requires them to remove such electronic protection.

Although this **does not constitute an exception** to an obligation to unencrypt end-to-end encryption, its technical unfeasibility would seem to make it **unlikely that a TCN requiring such a measure in relation to specific data would be issued** to a telecommunications operator.

There is, however, evidence that the UK Government will not hesitate to make a broader technical order to provide for longer-term backdoor access to otherwise encrypted data. This would not be to require a telecommunications operator to unencrypt particular end-to-end encrypted data, but rather to demand **systemic changes by the operator to remove end-to-end encryption protocol**. This would be with a view to allow for ongoing access to secure data in the event, for example, that there was a risk to national security.

It was **reported in early 2025 that the UK Government had issued Apple with a TCN demanding the right to access certain encrypted data** (namely end-to-end encrypted iCloud backups) from its users worldwide.[299] Similar to WhatsApp, Apple stated that it cannot view the data of customers who have activated its encryption tool, Advanced Data Protection (ADP), which prevents anyone other than the user from reading their files. To do so, it said, would have meant breaching its own encryption methods. In response to the TCN, Apple withdrew its ADP system for users in the UK, thereby removing the option to store data using end-to-end encryption. Apple also launched a legal process to challenge the TCN, which was due to be heard at a tribunal in early 2026. Latest reports in August 2025 say that the **UK has since withdrawn the TCN**, although no formal confirmation of this has been received by Apple.[300]

---

298 WhatsApp, *About government requests for user data*, available at https://faq.whatsapp.com/808280033839222 (27.08.2025).

299 BBC, *UK demands access to Apple users' encrypted data*, 7 February 2025, available at https://www.bbc.com/news/articles/c20g288yldko (28.08.2025).

300 See BBC, *UK backs down in Apple privacy row, US says*, 19 August 2025, available at https://www.bbc.com/news/articles/cdj2m3rrk74o (28.08.2025).

I. UNITED STATES

Introduction: Telecommunications and Government Surveillance

This section summarizes the mandatory and discretionary actions that certain telecommunications entities in the United States (US) must take in order to facilitate governmental surveillance activities.[301] In brief, the US adopts a decentralized, function-based approach to telecommunications surveillance. Providers are generally categorized by the nature of the services they offer—such as transmission, storage, or facilitation of communications. The U.S. legal system does not impose general obligations to pre-configure systems for surveillance (though it does impose such a requirement for some entities) or to retain data proactively. Instead, it primarily relies on provider cooperation in response to specific legal process, with obligations varying depending on the type of information sought and the nature of the investigation.

The key federal statutes governing these obligations are outlined immediately below and are developed further in the ensuing sections.[302]

- **Communications Assistance for Law Enforcement Act (CALEA)** – Enacted in 1994, CALEA, which is administered by the Federal Communications Commission (FCC), requires telecommunications carriers and manufacturers of telecommunications equipment design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities to comply with legal requests for information. In 2005, the FCC extended coverage of CALEA to include facilities-based broadband Internet access providers and providers of interconnected Voice over Internet Protocol (VoIP) service.
- **Stored Communications Act (SCA) –** The SCA, enacted in 1986 as part of the Electronic Communications Privacy Act (ECPA), governs access to stored electronic communications and associated data held by providers of Electronic Communication Services (ECS) and Remote Computing Services (RCS). The SCA prohibits providers from sharing electronic communications with any person or entity. However, it also contains exceptions, such as when the government compels the information. The SCA governs electronic communications and records "at rest" or in electronic storage held by providers. Other provisions of ECPA, such as the Wiretap Act, address communications in transmission.[303]
- **Pen Register and Trap and Trace Statute** - This statute, codified at 18 U.S.C. §§ 3121-3127, sets parameters for use of "pen registers" (which is a device or process that traces *outgoing* signals from a specific phone or computer to their destination)[304] and "trap and trace" devices (which captures *incoming* information (e.g., the source of a communication). These devices differ from a "wiretap", which records actual contents of telephone, email or other oral/written communications. This distinction has led to different standards for obtaining

---

301 These actions may include providing data, enabling access, or retaining information. The summary is primarily responsive to questions posed by the Swiss Federal Department of Justice and Police, some of which invite comparison with Swiss law. While no direct comparison is undertaken here, the section is designed to furnish a clear account of the US legal framework such that a reader familiar with the relevant provisions of Swiss law could draw their own comparisons.

302 While these federal statutes provide baseline protections for certain vulnerable classes, state law(s) sometimes provide more expansive protections. Notably, some states have included additional protected classes, relative to those set forth in the FHA. This will be discussed in greater detail in the context of the hypothetical scenarios.

303 For a good summary of selected SCA provisions that govern government request for electronic information from third parties, see https://www.congress.gov/crs-product/LSB10801.

304 See, https://www.law.cornell.edu/wex/pen_register.

authorization.[305] Notably, 18 U.S.C. 3123 allows a specific exception for companies that provide phone or internet services. These companies may utilize pen registers or trap and trace devices without prior authorization for certain enumerated purposes.[306]

- **Foreign Intelligence Surveillance Act (FISA) -** Originally enacted in 1978, FISA provides the framework for U.S. government surveillance conducted for foreign intelligence purposes, including electronic surveillance, physical searches, and compelled disclosure of records from service providers. Surveillance under FISA is overseen by the Foreign Intelligence Surveillance Court (FISC), which authorizes activities such as targeted collection of communications under Section 702. Importantly, Section 702 also imposes limitations on spying on American citizens. While FISA allows targeting non-US persons reasonably believed to be outside the US, in prohibits targeting US persons. Incidental collection of communications between a targeted foreigner and a US person can occur, but there are restrictions on how this data can be accessed and used.
- **Patriot Act and USA Freedom Act:** The **PATRIOT Act built on FISA,** expanding the U.S. government's surveillance reach in the name of counterterrorism after the events of September 11, 2001. The USA FREEDOM Act, passed in 2015, sought to reassert limits on those powers, reinforce constitutional protections, and restore public trust after disclosures of bulk surveillance. Notably, it ended bulk telephony metadata collection under Section 215 and requires the government to obtain a targeted warrant to collect phone records, while also increasing transparency at the Foreign Intelligence Surveillance Court (FISC).

1. How does the US classify telecommunication providers in the context of surveillance-centric regulations?

As noted above, CALEA is one of the most relevant statutes for understanding the rights and responsibilities of telecommunications providers relating to the facilitation of government surveillance activities. CALEA principally applies obligations to "telecommunications carriers", though over time the scope of CALEA has been extended to cover certain broadband and VoIP providers as well. To the extent that there are questions about which entities are (or are not) to be considered 'telecommunications carriers', the FCC, which has been granted a degree of regulatory authority under CALEA, makes those determinations.

1.1. CALEA

1.1.1. Telecommunications Carriers

Under CALEA, obligations to facilitate government surveillance activities largely relate to whether one is considered a "telecommunications carrier". This term is defined in 47 U.S.C. § 1001(8) as an entity "engaged in the transmission or switching of wire or electronic communications as a common carrier for hire." The statutory definition encompasses traditional telecommunications service providers, such

---

305 For a wiretap, the investigative authority must obtain a warrant, issued on the basis of there being "probable cause". Courts typically find there to be probable cause when there is a reasonable basis for believing that a crime may have been committed (for an arrest) or when evidence of the crime is present in the place to be searched (for a search). Authorization for a pen register or trap and trace device, will be given by a court if 'the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.' See 18 USCA § 3123.

306 These include: managing, maintaining or testing their service(s), protecting their rights or property, if the person using the service agrees to it, and others.

as AT&T, Verizon, or regional landline companies, which offer switched voice services over the public switched telephone network (PSTN).[307]

Moreover, and in recognition of technological convergence, the FCC exercised its rulemaking authority under 47 U.S.C. § 229(a) and CALEA Section 102(8)(B)(ii) to issue a 2005 First Report and Order, [308] which extended the definition to cover two additional categories of providers based on functional equivalence to traditional telephones:

- **Facilities-Based Broadband Internet Access Providers**: These are entities that own or operate the physical infrastructure over which broadband access is provided.[309]
- **Interconnected VoIP Providers**: These providers enable two-way, real-time voice communications over the internet and allow users to originate and terminate calls to and from the PSTN. The FCC defined "interconnected VoIP" as requiring a broadband connection, using IP protocols, and permitting interconnection with the traditional phone system.

The FCC emphasized that the applicability of CALEA to these entities is justified under the statute's "substantial replacement provision" (47 U.S.C. § 1001(8)(B)(ii)), which brings within CALEA's scope any service that is a replacement for a substantial portion of the local telephone exchange service.

1.1.2 Excluded entities

CALEA expressly excludes "information services" from its scope under 47 U.S.C. § 1001(8)(C)(i).[310] This carve-out encompasses services that offer "the capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications." As a result, email providers, cloud storage services, instant messaging platforms, and non-interconnected VoIP applications (e.g., Signal) are generally not subject to CALEA's interception capability requirements (see Section 3).[311] These services may still be subject to obligations under

---

307 Hurwitz, Justin. "EncryptionCongressmod (Apple+ CALEA)." Harv. JL & Tech. 30 (2016): 355, 419.

308 Under 47 U.S.C. § 229(a), Congress directed the FCC to prescribe such rules as are necessary to implement CALEA. Interestingly, In a January 16, 2025 Declaratory Ruling, the FCC under Chair Rosenworcel, concluded that Section 105 of CALEA imposes a general obligation on telecommunications carriers to secure their networks *against* unlawful access or interception—not just to facilitate lawful surveillance. It found that carriers must implement baseline cybersecurity measures (e.g., access controls, password protocols, patching vulnerabilities) and signaled intent to use CALEA as a foundation for expanded cybersecurity regulation, complemented by a related Notice of Proposed Rulemaking. It remains to be seen whether the FCC will continue with this stance, now that is led by the GOP. See. https://docs.fcc.gov/public/attachments/FCC-25-9A1.pdf

309 Even though broadband access has been identified by the FCC as an "information service" under the Communications Act (47 U.S.C. §§ 151–624), the FCC ruled that this classification does not exempt providers from CALEA because the Act defines its own categories.

310 The term "information services is defined in 47 U.S. Code § 1001(6). It states The term "information services"—
(A)means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and
(B)includes— (i)a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities; (ii)electronic publishing; and (iii)electronic messaging services; but
(C)does not include any capability for a telecommunications carrier's internal management, control, or operation of its telecommunications network.

311 Apparently three is some dispute as to whether SMS/MMS is subject to CALEA. See, for example, https://www.subsentio.com/is-rich-communication-service-subject-to-the-calea-lawful-surveillance-statute/

other statutes, such as the Stored Communications Act or the Foreign Intelligence Surveillance Act, but they are not required to design systems that are surveillance-capable under CALEA.

1.2. SCA

The classifications of "Electronic Communication Service" (ECS) and "Remote Computing Service" (RCS) are important concepts in U.S. surveillance law, particularly under the Stored Communications Act (SCA), which is Title II of the Electronic Communications Privacy Act of 1986 (ECPA) (codified at 18 U.S.C. §§ 2701–2712).

According to §2510(15), an ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications." This would tend to encapsulate email services, messaging services and telecommunications carriers (e.g., when handling stored voicemails or SMS).[312] An RCS, defined in §2711(2), is "The provision to the public of computer storage or processing services by means of an electronic communications system." Examples from case law include, a computer bulletin board service and YouTube were both considered RCS. [313]

As will be detailed in Section 3, below, these categories determine what obligations a given service provider has, what kinds of data the government can access, and what legal process (e.g., subpoena, court order, warrant) is required to compel that access.

2. What surveillance and information obligations do telecommunication service providers have in the US?

2.1. Obligations of Covered Entities (i.e., Telecommunications Carriers) Under CALEA

Entities covered by CALEA (i.e., telecommunications carriers) must ensure that their equipment, facilities, and services are capable of enabling law enforcement to conduct lawful intercepts. According to 47 U.S.C. § 1002(a),[314] a covered entity must be able, "in a manner that protects the privacy and security of communications not authorized to be intercepted, and without interfering with the services that the carrier provides," to:

(1) expeditiously isolate and enable the government, pursuant to a court order or other lawful authorization intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government.

(2) expeditiously isolate and enable the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier.

---

312 See generally, https://canons.sog.unc.edu/2012/04/outsourcing-local-government-communications-implications-of-the-federal-stored-communications-act/

313 See *Steve Jackson Games, Inc. v. U.S. Secret Service,* 816 F.Supp. 432, (W.D.Tex. 1993) affirmed 36 F.3d 457 and *Viacom v. YouTube,* 2008 WL 2627388 (S.D.N.Y. 2008).

314 Notably, the same section contemplates the carrier 'delivering' requested materials to the government. This would suggest that access to the data is mediated and controlled by the provider.

(3) deliver intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and

(4) facilitate authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects: (A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and (B) information regarding the government's interception of communications and access to call-identifying information.

Importantly, CALEA does not require providers to decrypt communications where they do not possess the encryption keys (47 U.S.C. § 1002(b)(3)) and does not mandate the creation or retention of any communication or metadata that is not already generated by the system in the normal course of business.

Additionally, telecommunications carriers must file and maintain up-to-date System Security and Integrity (SSI) plans with the Commission, as those plans are described in the Code of Federal Regulations (in particular, 47 C.F.R. § 1.20005).[315]

2.2. Obligations under the SCA

Under the SCA, the obligations of a provider depend on whether it is classified as an Electronic Communication Service (ECS) or a Remote Computing Service (RCS)—two statutory categories that govern access to stored communications and associated data.

If a provider is classified as an ECS, law enforcement may obtain access to communications in "electronic storage" under § 2703(a). The type of legal process required depends on the age of the data:

- For emails or communications 180 days old or less, a search warrant based on probable cause is required.
- For communications older than 180 days, the government may obtain access using a subpoena with prior notice to the subscriber, or a court order under § 2703(d). This structure seems to reflect the statute's original assumption that older emails were likely to have been deleted/expunged. However, that assumption has become increasingly outdated in an era of cloud-based storage and persistent access to emails across devices.

In addition, ECS providers may be required to comply with preservation requests under § 2703(f). Upon receiving such a request from a governmental entity, the provider must preserve specified data for 90 days, renewable once, even if the government has not yet obtained the requisite legal process for access.

For RCS providers, the framework under § 2703(b) permits government access to stored content or metadata depending on the type of information sought and the legal process used. Content data may be disclosed pursuant to a warrant, a § 2703(d) court order, or a subpoena with prior notice, depending on the circumstances.

Importantly, the US Supreme Court's decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), has helped shape how courts apply these provisions in practice. In *Carpenter*, the Court held that

315 https://www.fcc.gov/calea

government acquisition of historical cell site location information (CSLI) over a period of seven days or more constitutes a Fourth Amendment search requiring a warrant supported by probable cause, even though the data was held by a third-party provider. While the decision did not invalidate any part of Section 2703, it arguably casts doubt on the sufficiency of subpoenas or § 2703(d) orders to obtain certain sensitive metadata—particularly where the data is revealing, location-based, or accumulated over time.

2.3. Obligations under FISA

The Foreign Intelligence Surveillance Act (FISA) is the primary U.S. statute governing government surveillance for foreign intelligence purposes, authorizing the collection of communications and other data with judicial oversight from the Foreign Intelligence Surveillance Court (FISC). While FISA does make mention of "Electronic Communication Service Providers" (ECSP),[316] it does not require ECSPs to redesign infrastructure, pre-install surveillance interfaces, or retain data absent an order. Technical compliance is case-specific, and assistance is compelled only once a lawful order has been issued.[317] The relevant statute does not seem to require the designation of a point person at the provider entity to facilitate governmental requests/demands for access.[318]

Surveillance under the Foreign Intelligence Surveillance Act (FISA) typically requires court orders from the Foreign Intelligence Surveillance Court (FISC).[319] However, some forms of surveillance—such as under Section 702—permit the warrantless collection of communications of non-US persons located abroad, subject to judicial oversight through general programmatic approvals.

3. How does the federal law in the US regulate data retention?

The SCA permits law enforcement to issue preservation requests for stored content and subscriber data for 90 days, renewable once.[320] However, US law does not mandate general data retention by providers, except for specific requirements (such as the FCC's rule requiring telephone billing data to be retained for 18 months[321]).

316 See 50 U.S.C. § 1881(b)(4) (FISA Section 702 context), where it defines an ECSP as "A telecommunications carrier, a provider of electronic communication service, a provider of remote computing service, or any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or while they are stored."

317 For a broad look at the mechanics of the Surveillance Program Operated Pursuant to Section 702 of FISA, see the report of The Privacy and Civil Liberties Oversight Board (PCLOB) - an independent federal agency that provides oversight and analysis of U.S. intelligence and counterterrorism programs - found here: https://documents.pclob.gov/prod/Documents/OversightReport/e9e72454-4156-49b9-961a-855706216063/2023%20PCLOB%20702%20Report%20%28002%29.pdf?utm

318 Id,

319 *Foreign Intelligence Surveillance Act* (FISA) Citation: 50 U.S.C. §§ 1801–1885c.

320 See 18 U.S.C. § 2703(f)

321 47 CFR § 42.6 - Retention of telephone toll records

A proposed mandatory data retention law (e.g., the Data Retention Act)[322] has been considered in the past but has not been enacted. The more general trends in the US have been to emphasize privacy interests in digital data, contributing to provider caution about long-term retention.[323]

4. How does the law regulate the retention of boundary data ("Randdaten")?

US law does not impose any general obligation on communications providers to retain boundary data[324]. Instead, the retention and handling of such data are largely left to the discretion of individual service providers, guided by business needs, network management practices, and—increasingly—consumer privacy expectations.

Importantly, boundary data in the US is not treated as a protected category requiring heightened safeguards, nor is it designated for mandatory retention for law enforcement purposes (see Section 6 below). Rather, the legal regime governing boundary data access is primarily procedural and reactive. Law enforcement agencies can obtain such data from providers under various forms of legal process, depending on the sensitivity of the information and the type of provider. For instance, under the Pen Register and Trap and Trace Statute (18 U.S.C. §§ 3121–3127), the government can compel real-time access to signaling information (like dialed numbers or IP addresses) with a relatively low threshold court order—requiring only that the information be *relevant to* an ongoing investigation, rather than on the basis of probable cause.

When boundary data is stored—such as in email headers, connection logs, or IP address records—the SCA may apply. Under the SCA, law enforcement may obtain non-content metadata, including boundary data, with a subpoena or court order under 18 U.S.C. § 2703(d), depending on the context. However, nothing in the SCA requires providers to retain such data in the first place.

In sum, US law does not require the retention of boundary data, nor does it impose technical, or design requirements aimed at facilitating its collection. Instead, the law relies on provider-specific practices and targeted legal tools to access such data when needed, all within a framework that is increasingly attentive to the privacy implications of metadata surveillance.

5. How long must providers in the US retain data, according to federal law?

In the US, there is no overarching federal law that imposes a mandatory data retention period on telecommunications providers or internet-based service platform.[325] Instead, retention practices are

---

322 The Bill in question, HR 1981, was actually entitled the Protecting Children from Internet Pornographers Act but was often referred to informally as the Data Retention act. The Bill, which never received a full vote, would have required commercial ISPs to retain temporarily assigned IP address logs for at least 12 months.

323 Notably, some states (e.g., California) have enshrined rights to deletion and limits on storage duration.

324 "Boundary data" is understood here as technical transmission data such as IP addresses, email headers, call setup information, and other signaling metadata used to route or establish communications.

325 Note that some sectors (e.g., financial, healthcare) may face data retention requirements unrelated to telecom law. The ISDC has not conducted a full examination of these other sectors.

primarily shaped by providers' own business policies, technical constraints, and—increasingly—privacy considerations. As a result, retention periods can vary widely across sectors and companies.

The only statutory mechanism that allows the government to intervene in retention is the preservation order provision (18 U.S.C. § 2703(f)), which permits law enforcement to request that ECS and RCS providers to 'take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.' Such records must be retained for 90 days, renewable once.

There have been attempts to introduce federal mandatory retention laws—especially aimed at combatting child exploitation or enhancing counterterrorism efforts—but these proposals have consistently faced strong opposition from privacy advocates, the tech industry, and civil liberties organizations.

In short, there is no fixed retention period in US law, and the general tendency has been to avoid universal or preventive data retention mandates. Instead, the US relies on targeted, temporary preservation orders and provider discretion, with a growing emphasis on limiting data retention to protect individual privacy and reduce surveillance overreach.

Conclusion

In summary, while the US legal regime allows for targeted and legally authorized access to a wide array of communications and metadata, it stops short of mandating general-purpose surveillance infrastructure or long-term data retention—favoring a reactive, process-driven model that reflects constitutional and commercial considerations.

SWISS INSTITUTE OF COMPARATIVE LAW

Heckendorn Urscheler Lukas RLGPOZ

Signature numérique de Heckendorn Urscheler Lukas RLGPOZ
Date : 2025.10.02 15:58:06 +02'00'

Prof. Dr. Krista Nadakavukaren Schefer
Co-Head of Legal Division

Austria + Germany	Dr. Johanna Fournier, LL.M. *Legal Adviser, German-speaking Jurisdictions*
Denmark + Sweden	Henrik Westermark, LL.M *Legal Adviser, Scandinavian Jurisdictions*
France	Vaïtea Baillif *Legal Adviser, French-speaking Jurisdictions*
Russian Federation	Mariia Pribytkova *Legal Adviser, Eastern Jurisdictions*
Spain	Dr. Rodrigo Polanco Lazo *Legal Adviser, Spanish- and Portuguese-speaking Jurisdictions*
UK (England & Wales)	John Curran, LL.M *Legal Adviser, Common Law*
USA	Sean Stacy *Legal Adviser, US Law and Common Law*