EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

November 2022 Update

Country: France

FRANET contractor: French Institute for Human Rights and Civil Liberties

Reviewed by M. Lafourcade

Table of Contents

1. Summary

*FRANET contractors are requested to highlight in 1 page **maximum** the key developments in the area of surveillance by intelligence services in their Member State. This introductory summary should enable the reader to have a snapshot of the evolution during the reporting period (mid-2016 until third quarter of 2022). It should mention:*

the most significant legislative reform/s that took place or are taking place and highlight the key aspect/s of the reform, focusing on oversight and remedies.
relevant oversight bodies' (expert bodies (including non-judicial bodies, where relevant), data protection authorities, parliamentary commissions) reports/statements about the national legal framework in the area of surveillance by intelligence services.

List of the different relevant reports produced in the context of FRA's surveillance project to be taken into account

FRA 2017 Report:
Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update

FRANET data collection for the FRA 2017 Report:
Country studies for the project on National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies - Legal update

Country studies for the project on National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies - Monthly data collection on the current reform of intelligence legislation (BE, FI, FR, DE, NL and SE)

FRA 2015 Report:
Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – mapping Member States' legal framework

FRANET data collection for the FRA 2015 Report:
Country studies for the project on National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

A. Legislative reforms

I. The decree of 14 June 2017 amended the Code for defence (*code de la défense*) to substitute the national intelligence coordinator for the national coordinator for intelligence and counter-terrorism (*coordonnateur national du renseignement et de la lutte contre le terrorisme*).[1] Appointed by decree by the council of ministers (*conseil des ministres*), this national coordinator is responsible for the overall analysis of the threat and providing the President of the Republic with guidelines for intelligence and counter-terrorism, and the priorities for coordinated action, which he sets for the services. With the ministries involved, this national coordinator coordinates and develops the initiatives taken by France in terms of European and international cooperation in the fields of intelligence.

The national coordinator for intelligence and counter-terrorism (*coordonnateur national du renseignement et de la lutte contre le terrorisme*) ensures the proper cooperation of the

[1] France, Code for defence (*Code de la défense*), Article R*1122-7.

specialized intelligence services[2] and other intelligence services[3] in order to promote the sharing of information and the effectiveness of action, in particular faced with the terrorist threat. The national coordinator ensures the coordination of these services between ministries. Within each ministry, the national coordinator ensures the setting up and effectiveness, under the authority of each minister, of internal coordination and information sharing mechanisms. The national coordinator promotes the pooling of technological resources between specialized services. The heads of the intelligence services provide the national coordinator with the information to be brought to the attention of the President of the Republic and the Prime Minister and report to him on their activities.[4]

With the assistance of the Secretary General for defence and national security (*secrétaire général de la défense et de la sécurité nationale*), the national coordinator for intelligence and counter-terrorism reports to the national defence and security council (*conseil de défense et de sécurité nationale*) and to the national intelligence council (*conseil national du renseignement*). The national coordinator prepares the meetings of the latter. He follows up on the implementing of decisions relating the intelligence services taken in these bodies.[5]

The national coordination for intelligence and counter-terrorism (*coordination nationale du renseignement et de la lutte contre le terrorisme*) is placed under the authority of the national coordinator for intelligence and counter-terrorism.[6] The national counter-terrorism centre (*centre national de contre-terrorisme*) is part of the coordination, and is responsible for analysing the threat and the counter-terrorism strategy.[7] The national coordination for intelligence and counter-terrorism (*coordination nationale du renseignement et de la lutte contre le terrorisme*) is a member of the French intelligence community (*communauté française du renseignement*) since 2017.[8]

The decree also allowed the intelligence services inspectorate (*inspection des services de renseignement*) to carry out monitoring, audit, study, advisory and assessment assignments with respect to the other intelligence services referred to in Article R. 811-2 of the Internal Security Code (*code de la sécurité intérieure*).

II. The law of 30 October 2017 strengthening internal security and counter-terrorism introduced a new legal regime for monitoring certain wireless communications after the Constitutional Court (*Conseil constitutionnel*) ruled that such a surveillance should be subject to review.[9] Now the intelligence services have to request the authorisation to intercept and make use of private communications that are exclusively wireless and that do not involve the

[2] France, Internal Security code (*Code de la sécurité intérieure*), Article R. 811-1.
3 France, Internal Security code (*Code de la sécurité intérieure*), Article R. 811-2.
[4] France, Code for defence (*Code de la défense*), Article R. * 1122-8-1.
[5] France, Code for defence (*Code de la défense*), Article R. * 1122-8.
[6] France, Code for defence (*Code de la défense*), Article R. * 1122-8-2.
[7] France, Code for defence (*Code de la défense*), Article R. * 1122-8-2.
[8] France, Internal Security code (*Code de la sécurité intérieure*), Article R 811-1.
[9] France, Constitutional Council (*Conseil constitutionel*), Decision 2016-590 QPC, 21 October 2016, available at : www.conseil-constitutionnel.fr/decision/2016/2016590QPC.htm#:~:text=LE%20CONSEIL%20CONSTITUTIONNEL%20A%20%C3%89T%C3%89,une%20question%20prioritaire%20de%20constitutionnalit%C3%A9.

action of an electronic communications operator: the Prime minister may not grant such a warrant without obtaining beforehand the legal opinion of the CNCTR, as required by law for any other intelligence technique. When authorised, its implementation is then subject to *ex post* verifications by the CNCTR.

When the interception does not target private communications within a wireless network, such as communications intercepted for military defence or maritime safety needs, prior authorisation is not required by law but the CNCTR must perform *ex post* verifications on such monitoring.

The information collected is then destroyed after a period of six years from the date of collection. For items of information that are encrypted, the time limit runs from the moment they are decrypted. They may not be kept for more than eight years from the date of their collection.

This information may not be transcribed or extracted for any purpose other than the following: national independence, territorial integrity and national defence; the major interests of foreign policy, the fulfilment of France's European and international commitments and the prevention of any form of foreign interference; France's major economic, industrial and scientific interests; the prevention of terrorism; the prevention of attacks on the republican form of institutions; actions tending to the maintaining or reconstituting of groups dissolved pursuant to Article L. 212-1 of the Internal security code; collective violence likely to seriously undermine public order; prevention of organized crime and delinquency; the prevention of the proliferation of weapons of mass destruction.[10] Transcripts or extracts must be destroyed as soon as their retention is no longer essential for the pursuit of these purposes.

The CNCTR is informed of the scope and type of the measures taken and may, at its request and for the sole purpose of ensuring compliance with the scope of application, be shown on the spot the interception capabilities implemented and be provided with the information collected and kept on the date it was requested and the transcriptions and extractions made. The CNCTR may also make recommendations and observations to the Prime Minister and the DPR that it deems to be needed in the context of the monitoring it exercises.

The law perpetuates the regime that allows the consultation of the data of air transport passenger records. It creates a national system for centralising maritime transport passenger records.

III. The law of 13 July 2018 on military planning for the period 2019-2025 completed the legal framework for the surveillance of international electronic communications and strengthened the CNCTR's powers in this area.

Use of international electronic communications must now be subject to prior review by the CNCTR and can be done only for the aims listed in Article L811-3 of the Internal Security code.[11]

[10] France, Internal Security code (*Code de la sécurité intérieure*), Article L. 811-3.
[11] France, Internal Security code (*Code de la sécurité intérieure*), Article L. 811-3. See also this list in II.

The number of authorizations granted to intercept international electronic communications of a person using a French subscriber's number from the French territory is subject to a quota set by the Prime minister after receiving the CNCTR's opinion.

IV. The law of 30 July 2021 on intelligence and the prevention of acts of terrorism strengthens the 2015 intelligence law by taking changes in technologies and communication methods into account.

a) Interception of satellite communications[12]

The intelligence services have new monitoring facilities, including the possibility, on an experimental basis, up to 31 July 2025, to intercept satellite communications in order to protect national independence, territorial integrity and national defence; the major interests of foreign policy, the fulfilment of France's European and international commitments and the prevention of any form of foreign interference; the prevention of terrorism and prevention of organized crime and delinquency.[13]

The authorisation to intercept satellite communications will be granted by the Prime Minister, on the basis of opinion from the National commission for the control of intelligence techniques (*Commission nationale de contrôle des techniques de renseignement* - CNCTR), for a period of up to 30 days.

A service of the Prime Minister (*Groupement Interministériel de Contrôle*, GIC),[14] which is not an intelligence service, organises the centralising of intercepted correspondence and the information or documents collected. The transcription and extraction of intercepted communications, to which the CNCTR will have "continuous, complete, direct and immediate" access, are also carried out within GIC. GIC then makes this data available to the intelligence services and monitors their use. Intercepted ccorrespondence is destroyed as soon as it becomes apparent that it has no connection with the person involved by the authorisation issued. The maximum period of retention of the collected data relating to the person under surveillance is limited to thirty days. The Prime Minister sets up the maximum number of simultaneous authorizations to intercept, after consulting the CNCTR.

b) Technical algorithm [15]

The so-called technical algorithm, which has been tested since 2015 and was authorised up to 31 December 2021, has been made permanent. This technique allows automated processing of Internet connection and browsing data, through the cooperation of access providers. Only the specialized intelligence services referred to in Article L. 811-2 of the Internal Security Code (*Code de la sécurité intérieure*) can request authorisation to implement algorithms for the sole purpose to detect communications data that would reveal a terrorist threat. The service of the Prime minister is alone authorised to carry out this processing and these operations, under the supervision of the CNCTR, which reviews *ex ante* any request for implementing such a technique. Moreover, the relevant intelligence service must request the approval of the Prime minister to access and identify communication data that has been detected through this

[12] France, Internal Security code (*Code de la sécurité intérieure*), Article L. 852-3.
[13] France, Internal Security code (*Code de la sécurité intérieure*), Article L. 811-3.
[14] France, Internal Security code (*Code de la sécurité intérieure*), Article R 823-1.
[15] France, Internal Security code (*Code de la sécurité intérieure*), Article L 851-3.

technique. He may not grant any warrant without obtaining beforehand the legal opinion by the CNCTR.

Data revealing a terrorist threat must be treated within 60 days and then destroyed. Data collected that does not reveal a threat has to be destroyed immediately. This algorithm-based monitoring is extended to Internet connection addresses (URLs). The members of the National Assembly (*Assemblée nationale*) have required the government to submit an initial report on the monitoring of URLs by mid-2024 at the latest.

c) URL collected in real time [16]

The law of 30 July 2021 on intelligence and the prevention of acts of terrorism authorised the real-time collection of "the complete addresses of Internet resources used" by previously identified persons likely to be associated with a terrorist threat, and by anyone else around them.

d) Sharing of information between the intelligence services and with administrative authorities

The "first circle"[17] and "second circle"[18] services which obtain information useful for pursuing a purpose other from that which justified their collection, may henceforth transcribe or extract such information for carrying out their duties and forward it to another first or second circle service "provided such forwarding is strictly necessary for carrying out the duties of the recipient service". Sharing information is subject to prior authorisation by the Prime Minister on the basis of opinion from the CNCTR when the forwarding of collected information is for a purpose other than the one that justified its collection or if the information is derived from the implementing of an intelligence gathering technique that the recipient service could not have used for the purpose for which it was forwarded.[19] This transmission must be also strictly necessary for the performance of the missions of the recipient service, and be within the limits of the purposes mentioned in Article L. 811-3 of the Internal Security code, listed above.

The law of 30 July 2021, which takes into account the decision of the Constitutional Council (*Conseil constitutionnel*) of 9 July 2021,[20] removes the possibility for administrative authorities to forward information to the intelligence services on their own initiative. However, administrative authorities may transmit information to the specialized intelligence services at

[16] France, Internal Security code (*Code de la sécurité intérieure*), Article L 851-2.
[17] This refers to the directorate general of foreign security (*direction générale de la sécurité extérieure* - DGSE), the directorate of defence intelligence and security (*direction du renseignement et de la sécurité de la défense* - DRSD), the directorate of military intelligence (*direction du renseignement militaire* - DRM), the directorate general of homeland security (*direction générale de la sécurité intérieure* - DGSI), the national directorate of customs intelligence and investigations (*direction nationale du renseignement et des enquêtes douanières* - DNDRED) and the processing of intelligence and action against clandestine financial circuits (*traitement du renseignement et action contre les circuits financiers clandestins* - TRACFIN).
[18] The "second circle" departments are designated by decree of the Council of State (*Conseil d'État*) on the basis of opinion from the CNCTR. They include specialised intelligence services such as the central service for regional intelligence (*service central du renseignement territorial* - SCRT) or the intelligence directorate of the Paris police prefecture (*direction du renseignement de la préfecture de police de Paris* - DRPP).
[19] France, Internal Security code (*Code de la sécurité intérieure*), Article L 822-3.
[20] The Internal Security code allowed administrative authorities to forward 'all useful' information to the intelligence services on their own initiative. The Constitutional Council considered this provision contrary to the Constitution as violating right to the respect of private life.

their request.[21] The law also provides a framework for the forwarding from administrative authorities to the intelligence services of so-called sensitive data, excluding the possibility of forwarding genetic data, and strengthens traceability requirements for all forwarding operations.[22]

e) Extension of retention and authorization periods

The retention period of collected data that may be used for research and development purposes has been extended to five years. The technical settings of these programmes will be subject to prior authorisation by the Prime Minister, issued on the basis of an opinion from the CNCTR.[23]

The authorisation period for the computerised data collection technique has been extended from 30 days to 2 months.[24]

The law has amended the provisions of Article L. 34-1 of the French Post and Electronic Communications Code (*Code des postes et des communications électroniques*) and of Article 6 of the French law of 21 June 2004 on confidence in the digital economy (*confiance dans l'économie numérique*), drawing the consequences of the decision of the French Data Network et al. of the French Council of State (*Conseil d'État*) of 21 April 2021 with regard to the rules applicable to communications operators, access providers and hosting companies for the retention of connection data. Electronic communications operators will be required to keep, for the purposes of criminal proceedings, the prevention of threats to public safety and the safeguarding of national security, information relating to the user's civil identity, up to the expiry of a period of 5 years from the end of their contract's validity. For the purposes of combating crime and serious delinquency, preventing serious threats to public safety and safeguarding national security, they will also be required to keep technical data identifying the connection source or data relating to the terminal equipment used, up to the expiry of a period of one year from the connection or use of the terminal equipment. In the event of a serious, current or foreseeable threat to national security, the Prime Minister may order electronic communications operators to keep, for a period of one year, certain categories of traffic data and location data, which will be specified by a Council of State (*Conseil d'État*) decree. The Prime Minister's order which may not exceed one year, may be renewed if the conditions for its issuance continue to be met. Finally, data kept by operators will be subject to a rapid retention order by authorities with access to electronic communications data, for the purpose of preventing and combating serious crime.

f) Assistance with Imsi-catcher devices

The law also broadens the scope of the intelligence techniques referred to in Article L. 871-6 of the Internal Security Code (*Code de la sécurité intérieure*) for which the administrative authority may request the assistance of electronic communications operators. It extends the possibilities of requisition to the implementing of an Imsi-catcher type proximity capture device.[25]

---

[21] France, Internal Security code (*Code de la sécurité intérieure*), Article L.863-2.
[22] France, Internal Security code (*Code de la sécurité intérieure*), Article L 863-2.
[23] France, Internal Security code (*Code de la sécurité intérieure*), Articles L 822-2 and 822-2-1.
[24] France, Internal Security code (*Code de la sécurité intérieure*), Article L853-2.
[25] France, Internal Security code (*Code de la sécurité intérieure*), Article L 851-6.

g) The strengthening of CNCTR's powers[26]

The CNCTR's prior monitoring of all intelligence techniques in France has been strengthened. The law now provides that in case of disagreement between the CNCTR and the Prime minister on any request for surveillance measure, the supreme court for administrative justice (*Conseil d'Etat*) should make the final decision. Should the authorisation of the Prime Minister be issued after a negative opinion from the CNCTR, the matter is immediately referred to the Council of State (*Conseil d'Etat*) by the chair of the commission and a decision is taken within twenty-four hours of this referral. The Prime Minister's authorisation decision may not be executed before the Council of State (*Conseil d'Etat*) has ruled, except in the case of a duly justified emergency and if the Prime Minister has ordered its immediate implementation.

h) The strengthening of the parliamentary delegation for intelligence's powers[27]

The prerogatives of the parliamentary delegation for intelligence (*délégation parlementaire au renseignement* - DPR) have also been strengthened in terms of access to documents and other information through hearings of personalities exercising management duties within the intelligence services. Up to now, only the heads of the services and those placed under these heads and occupying a post filled by the Council of Ministers (*conseil des ministres*) could be heard. The DPR may now also request any document, information and assessment consideration needed to carry out its duties. However, this extended right to information remains limited to the DPR's need to know, thereby excluding ongoing operations, operational methods and the services' relations with their foreign partners.

The scope of the DPR has been extended to include the monitoring of current issues and future challenges to public intelligence policy. The DPR now receives, every six months, the list of inspection reports relating to the intelligence services.

Finally, DPR now has the option of requesting the national coordinator for intelligence and counter-terrorism once a year to submit the national intelligence guidance plan (*plan national d'orientation du renseignement*, PNOR).[28]

B. Oversight bodies' reports/statements about the national legal framework in the area of surveillance by intelligence services

2.1. In its Opinion on the bill to strengthen domestic security and counter-terrorism (which became the law of 30 October 2017), the National advisory commission for human rights (*Commision nationale consultative des droits de l'homme*, CNCDH), stressed that its measures enshrine the preponderance given by the government to security concerns and called on the

[26] France, Internal Security code (*Code de la sécurité intérieure*), Article L 821-1.
[27] France, Order No. 58-1100 on the functioning of parliamentary assemblies (*Ordonnance n° 58-1100 relative au fonctionnement des assemblées parlementaires*), 17 November 1958, Article 6 ninth.
[28] France, Parliamentary delegation for intelligence (*Délégation parlementaire au renseignement)*(2021), Report on the activities of the parliamentary delegation on intelligence for the year 2020-2021 *(Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2020-2021).*

government to abandon this bill insofar as it definitively incorporated the state of emergency into the legal order.

2.2. The National Commission for Informatics and Freedoms (*Commission Nationale de l'Informatique et des Libertés*, CNIL) issued three opinions dated 8 April,[29] 15 April,[30] and 3 May 2021,[31] on certain provisions of the bill on the prevention of terrorism, as then proposed by the Government. The CNIL did not have the information required to enable it to assess the need to perpetuate the so-called "algorithm" technique, as the detailed assessment was covered by national defence secrecy and was only accessible to the CNCTR and to the parliamentary delegation for intelligence (*délégation parlementaire au renseignement*). The CNIL considered it appropriate to carry out an experiment of the new intelligence technique allowing satellite interceptions and asked for an intermediate assessment to be made. It considered that the purposes justifying the implementing of this technique should be limited, in an experimental framework, to the public interest aims considered to be most compelling and most serious. With regard to other intelligence techniques, the CNIL noted that significant safeguards were implemented (such as limitations for certain purposes, retention periods and limited access), but recommended that additional safeguards (such as limitations on the purposes for which certain techniques could be used and clarification of the conditions for their implementation). The CNIL considered that monitoring the implementing of the law's provisions to be an essential guarantee in order to ensure that infringements of people's rights would be effectively limited to that strictly necessary.

2.3. The Parliamentary delegation for intelligence (*Délégation parlementaire au renseignement*), a joint body of the National Assembly (*Assemblée nationale*) and the Senate (*Sénat*), publishes annual reports on the results of its activities. In its 2020-2021 report, the delegation emphasised the need for increased and ongoing surveillance of social networks and called for the creation of a "national intelligence" directorate within the Ministry of the Interior to provide local intelligence services in order to deal with new risks to public order and prevent terrorism. The 2021-2022 report refers to the Pegasus case.

2.4. The CNCTR publishes annual reports regarding the results of its oversight activity over the intelligence services. The 2022 annual report emphasizes the new legal framework resulting from the law of July 31st, 2021.

[29] France, French Data Protection Authority (*Commission Nationale Informatique et Libertés, CNIL*), Resolution No. 2021-040 on a bill on intelligence and the prevention of acts of terrorism (*Délibération n° 2021-040 portant avis sur un projet de loi relatif à la prévention d'actes de terrorisme et au renseignement*), 8 April 2021.
[30] France, CNIL, Resolution No. 2021-045 on the opinion on Articles 13 second and 13 third of the bill on the prevention of acts of terrorism and on intelligence (*Délibération n° 2021-045 portant avis sur les articles 13 bis et 13 ter du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement*), 15 April 2021.
[31] France, CNIL, Deliberation No. 2021-053 on Articles 11 fifth, 11 sixth and 11 seventh of the bill on the prevention of terrorist acts and intelligence (*Délibération n° 2021-053 portant avis sur les articles 11 quinquies, 11 sexies et 11 septies du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement*), 3 May 2021.

2. Annexes- Table and Figures

2.1. Overview of security and intelligence services in the EU-27

FRANET contractors are requested to check the accuracy of the table below (see Annex pp. 93 - 95 of the FRA 2015 report) and correct or add in track changes any missing information concerning security and intelligence services in their Member State (incl. translation and abbreviation in the original language). Please provide the full reference in a footnote to the relevant national law substantiating all the corrections and/or addit[32]ions made in the table.

	Civil (internal)	Civil (external)	Civil (internal and external)	Military
FR[33]	Directorate General of Interior Security/ *Direction générale de la sécurité intérieure* (DGSI)	Directorate General of External Security/*Direction de la sécurité extérieure* (DGSE)	National coordination of intelligence and the fight against terrorism (*La coordination nationale du renseignement et de la lutte contre le terrorisme*, CNRLT) The national directorate of customs intelligence and investigation (*La direction nationale du renseignement et des enquêtes douanières*, DNRED) The "intelligence processing and action against clandestine financial circuits" department (*Le service " traitement du renseignement et action contre les circuits financiers clandestins "*, TRACFIN)	Directorate of Military Intelligence/ *Direction du renseignement militaire* (DRM) The Defence Intelligence and Security Directorate (*La direction du renseignement et de la sécurité de la défense*, DRSD)

2.2 EU Member States' legal framework on surveillance reformed since 2017

In order to update the map below (Figure 1 (p. 20) of the FRA 2017 report), FRANET contractors are requested to state:

[32] France, CNCTR (2021), Annual report, available at: www.cnctr.fr/6_relations.html#les-rapports-annuels-d-activite-de-la-cnctr.

[33] Table includes intelligence services of the first circle in France.

1. *Whether their legal framework on surveillance has been reformed or is in the process of being reformed since **mid-2017** – see the Index of the FRA 2017 report, pp. 148 - 151. Please do not to describe this new legislation but only provide a full reference.*

France, Decree No. 2017-1095 on the coordinator for national intelligence and counter-terrorism, the coordination of national intelligence and counter-terrorism (*Décret n° 2017-1095 relatif au coordonnateur national du renseignement et de la lutte contre le terrorisme, à la coordination nationale du renseignement et de la lutte contre le terrorisme et au centre national de contre-terrorisme*), 14 June 2017

France, Law strengthening internal security and counter-terrorism (*Loi n° 2017-1510 renforçant la sécurité intérieure et la lutte contre le terrorisme*), 30 October 2017

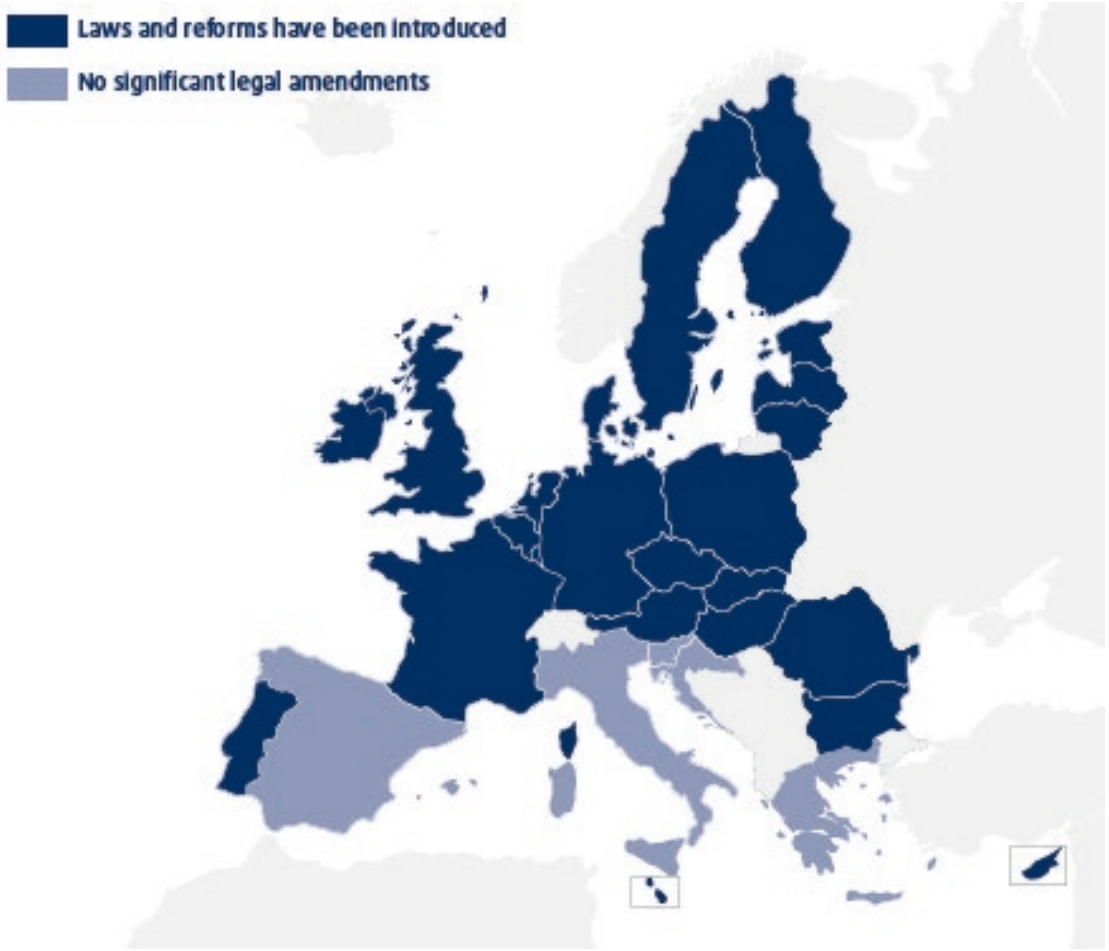
France, Law on military planning for the period 2019-2025 (*loi n° 2018-607 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense*), 13 July 2018

France, Law on the prevention of acts of terrorism and intelligence (*Loi n° 2021-998 relative à la prévention d'actes de terrorisme et au renseignement*), 30 July 2021

2. *whether the reform was initiated in the context of the PEGASUS revelations.*

No, but the investigations are pending.

Figure 1: EU Member States' legal frameworks on surveillance reformed since October 2015

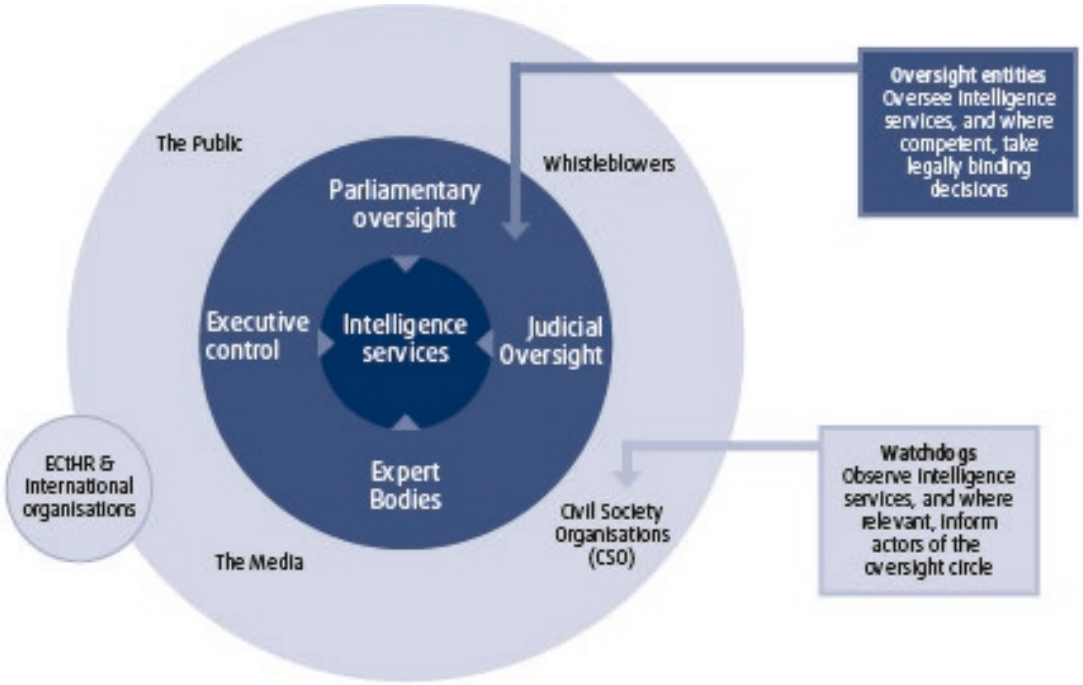


OK.

2.3 Intelligence services' accountability scheme

FRANET contractors are requested to confirm whether the diagram below (Figure 5 (p. 65) of the FRA 2017 report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

Figure 5: Intelligence services' accountability scheme

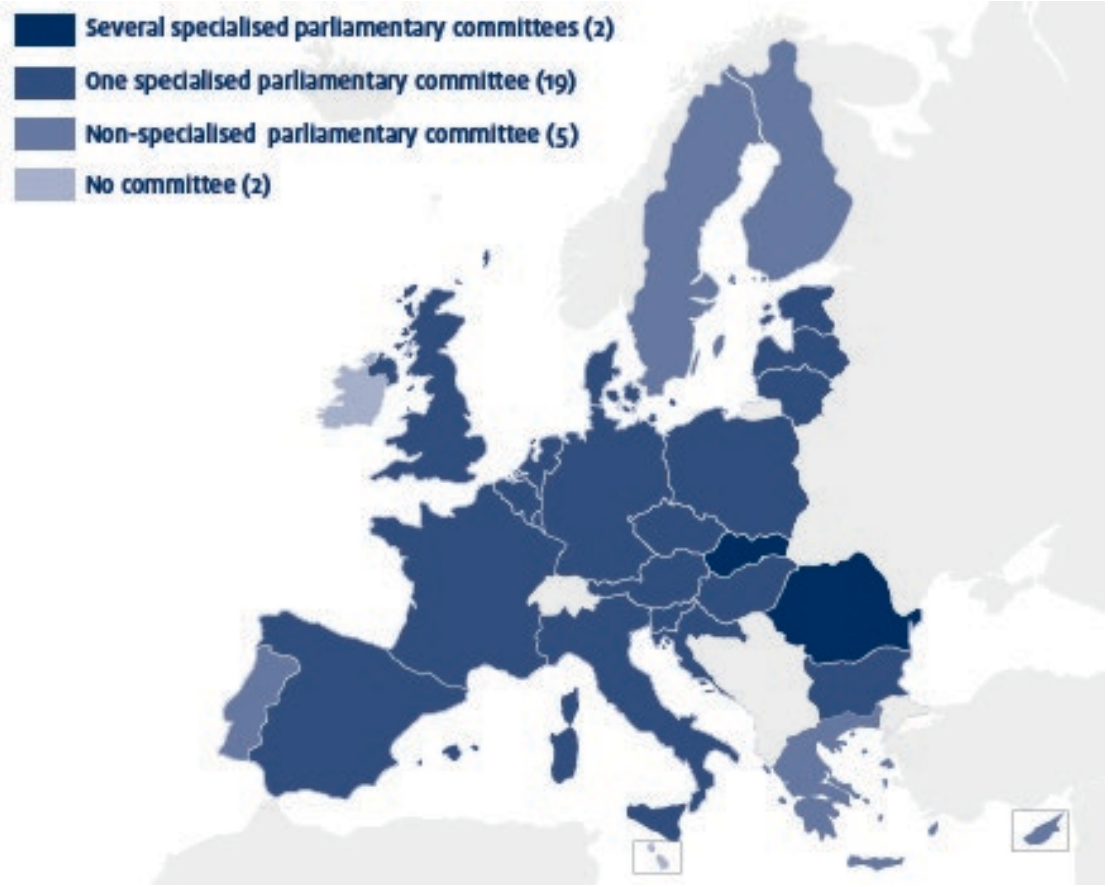


OK.

2.4 Parliamentary oversight of intelligence services in EU Member States

FRANET contractors are requested to confirm that the map below (Figure 6 (p. 66) of the FRA 2017 report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

Figure 6: Parliamentary oversight of intelligence services in EU Member States



YES, one specialized parliamentary committee.

2.5 Expert bodies (excluding DPAs) overseeing intelligence services in the EU

FRANET contractors are requested to check the accuracy of the table below (Table 2 (p. 68) of the FRA 2017 report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

Table 2: Expert bodies (excluding DPAs) overseeing intelligence services in the EU

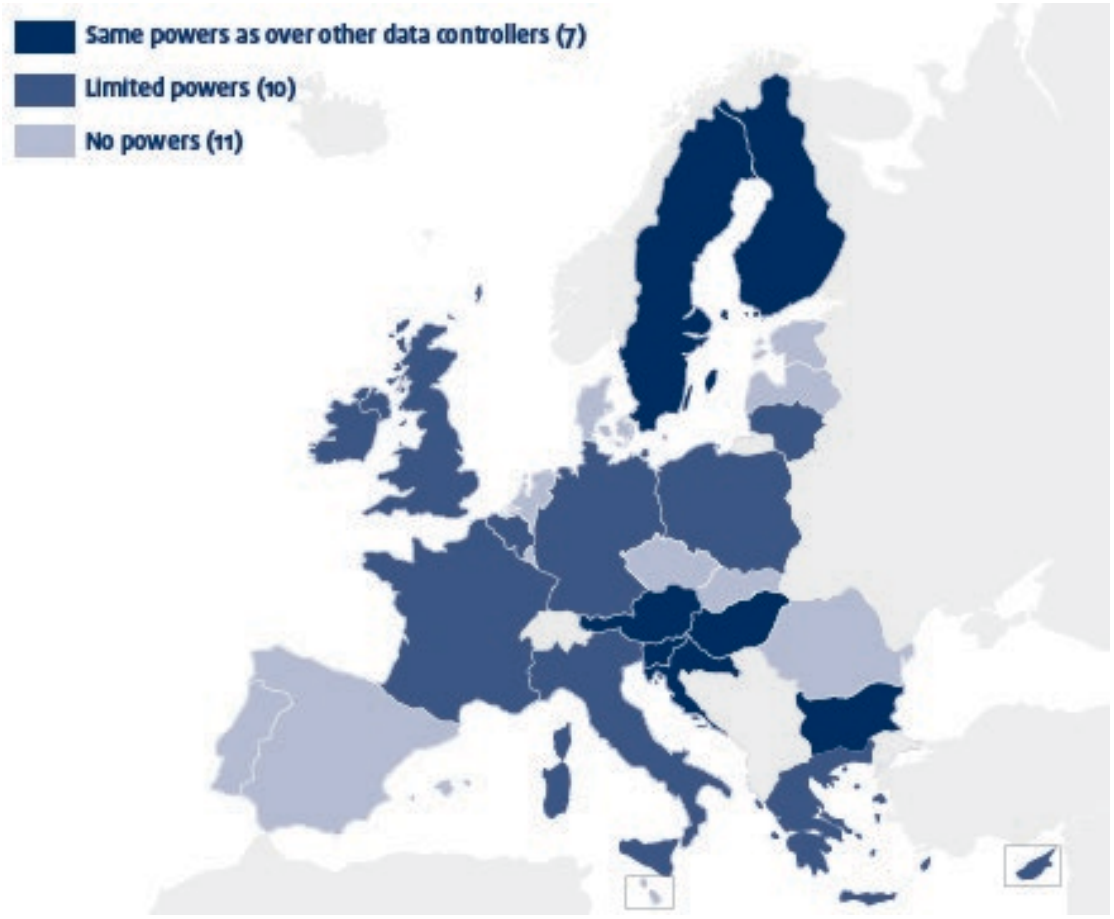
EU Member State	Expert Bodies
FR	National Commission for Control of Intelligence Techniques (*Commission nationale de contrôle des techniques de renseignement*) Council of State special formation

OK.

2.6 DPAs' powers over national intelligence services, by member states

FRANET contractors are requested to confirm that the map below (Figure 7 (p. 81) of the FRA 2017 report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

Figure 7: DPAs' powers over national intelligence services, by member states

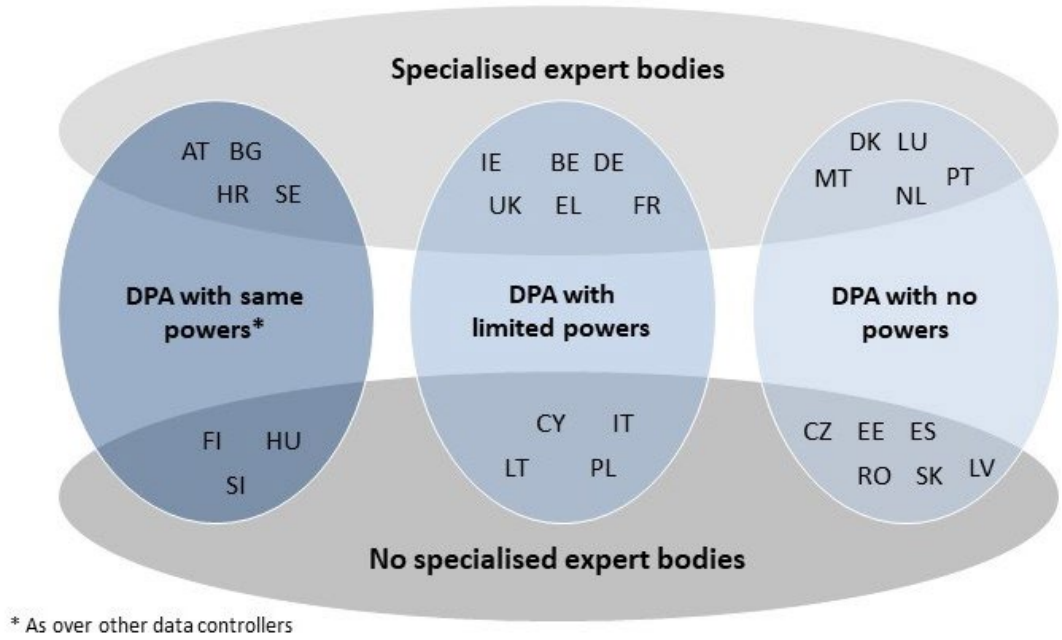


YES, limited powers (even if they were recently increased) Please refer to the section ***The strengthening of the parliamentary delegation for intelligence's powers.***

2.7 DPAs' and expert bodies' powers over intelligence techniques, by EU Member State

FRANET contractors are required to check the accuracy of the figure below (Figure 8 (p. 82) of the FRA 2017 report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

Figure 8: DPAs' and expert bodies' powers over intelligence techniques, by EU Member State



OK.

2.8 Binding authorisation/approval of targeted surveillance measures in the EU

FRANET contractors are required to check the accuracy of table below (Table 4 (p. 95) of the FRA 2017 report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

Table 4: Binding authorisation/approval of targeted surveillance measures in the EU-27

	Judicial	Executive	Expert bodies	Services
FR	✓	✓		

In the French new authorisation process, the Prime minister makes the decision after the CNCTR delivers an opinion. Should the Prime minister overrule a negative opinion, the CNCTR must then refer the case to the State Council, which makes the final decision.

2.9 Approval/authorisation of general surveillance of communication

All FRANET contractors are requested to check the accuracy of the table below (Table 5 (p. 97) of the FRA 2017 report), and to update/include information as it applies to their Member State (if not previously referred to). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework, in particular where - since 2017 - your Member State regulates these type of surveillance methods (for a definition of general surveillance, see FRA 2017 Report, p. 19).

Table 5: Approval/authorisation of general surveillance of communication in France, Germany, the Netherlands and Sweden

	Judicial	Parliamentary	Executive	Expert
FR	✓		✓	

In the French new authorisation process, the Prime minister make the decision after the CNCTR delivers an opinion. Should the Prime minister overrule a negative opinion, the CNCTR must then refer the case to the State Council, which make the final decision.

2.10 Non-judicial bodies with remedial powers

FRANET contractors are requested to check the accuracy of table below (Table 6 (p. 112) of the FRA 2017 report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

Table 6: Non-judicial bodies with remedial powers in the context of surveillance, by EU Member State

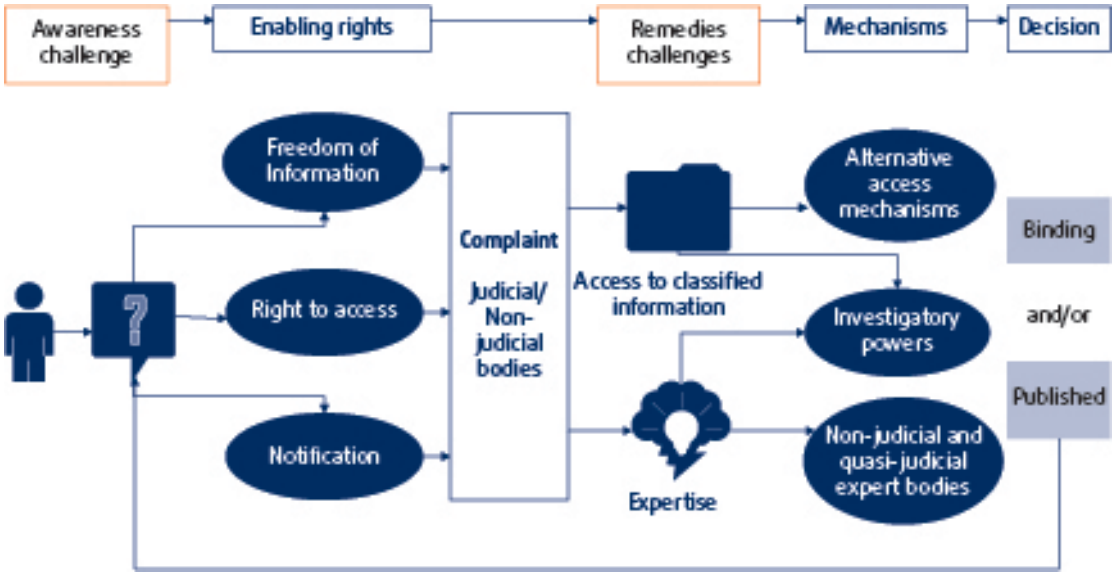
	Executive (ministry)	Expert body(ies)	DPA	Parliamentary committee(s)	Ombuds institution
FR		✓	✓		✓

OK.

2.11 Implementing effective remedies

FRANET contractors are requested to confirm that the diagram below (Figure 9 (p. 114) of the FRA 2017 report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

Figure 9: Implementing effective remedies: challenges and solutions



OK.

2.12 Non-judicial bodies' remedial powers

FRANET contractors are required to check the accuracy of table below (Table 7 (pp. 115 - 116) of the FRA 2017 report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

Table 7: Non-judicial bodies' remedial powers in case of surveillance, by EU Member State

	Bodies with remedial competence	Decisions are binding	May fully access collected data	Control is communicated to complainant	Decision may be reviewed
FR	National Commission for Control of Intelligence Techniques				
	Defender of Rights				
	National Commission on Informatics and Liberty				

Note:

= Expert body
= Ombuds institution
= Data protection authority
= Parliamentary Committee
= Executive

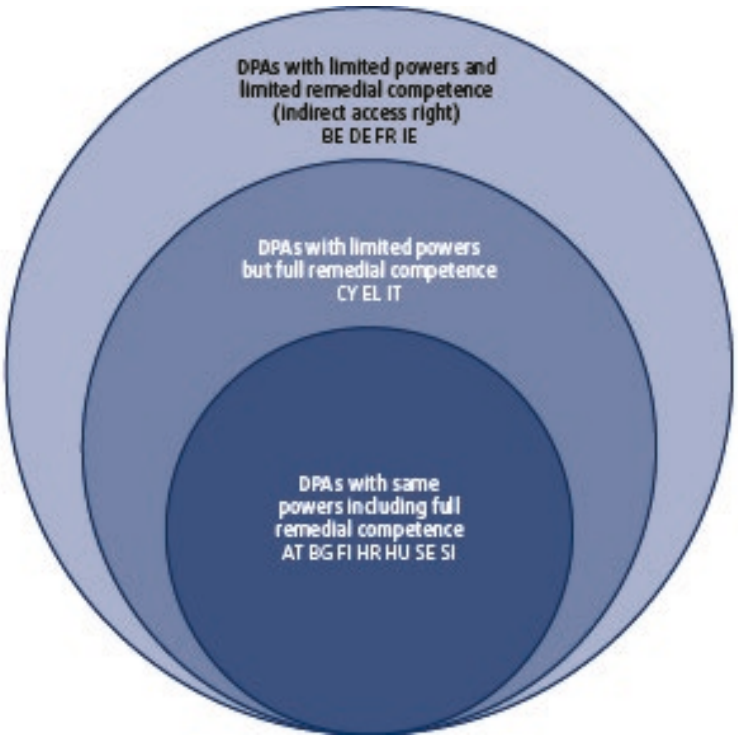
Source: FRA, 2017

Decisions rendered on individual complaints are binding for the parties.

2.13 DPAs' remedial competences

FRANET contractors are required to check the accuracy of the figure below (Figure 10 (p. 117) of the FRA 2017 report) with respect to the situation in your Member State. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

Figure 10: DPAs' remedial competences over intelligence services



OK.