الأمم المتحدة

A/HRC/46/37/Add.2

الجمعية العامة

Distr.: General
1 February 2021
Arabic
Original: English

مجلس حقوق الإنسان

الدورة السادسة والأربعون

22 شباط/فبراير – 19 آذار/مارس 2021

البند 3 من جدول الأعمال

تعزيز وحماية جميع حقوق الإنسان، المدنية والسياسية والاقتصادية والاجتماعية والثقافية، بما في ذلك الحق في التنمية

زيارة إلى فرنسا

تقرير المقرر الخاص المعني بالحق في الخصوصية، جوزيف أ. كاناتاتشي* **

موجز

أجرى المقرر الخاص المعني بالحق في الخصوصية، جوزيف أ. كاناتاتشي، زيارة رسمية إلى فرنسا في الفترة من 13 إلى 17 تشرين الثاني/نوفمبر 2017. وفي هذا التقرير، يسلط الضوء على المخاوف بشأن قوانين الطوارئ، ويوصي بمواصلة إصلاح القانون الفرنسي من أجل تكريس الصلاحيات الرقابية للجنة الوطنية لمراقبة تقنيات الاستخبارات ومواءمة الضمانات وسبل الانتصاف المطبقة فيما يخص الاستخبارات الأجنبية مع تلك المطلوبة فيما يخص الاستخبارات المحلية.

* يعمم موجز التقرير بجميع اللغات الرسمية. أما التقرير نفسه، المرفق بهذا الموجز، فيُعمم باللغة التي قُدّم بها وباللغة الفرنسية فقط.

** قُدم هذا التقرير بعد انقضاء الموعد النهائي لتضمينه أحدث المستجدات.

Annex

Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, on his visit to France

I. Introduction

1. The present report was finalized towards the end of 2020, after an evaluation of the preliminary results of the meetings held during the visit to France from 13 to 17 November 2017 and after having cross-checked those preliminary results against follow-up research and developments to date. The benchmarks used in the report include the privacy metrics set out in a draft document prepared in 2019 by the Special Rapporteur on the right to privacy, Joseph A. Cannataci.[1]

2. Much of the content of this report reflects and builds upon the findings already published in the end-of-mission statement published in November 2017.[2]

3. The Special Rapporteur thanks the Government of France for the open way in which it facilitated his visit. Discussions with government officials were held in a cordial, candid and productive atmosphere.

4. The Special Rapporteur thanks the representatives of civil society, urban police officers, government officials and other stakeholders who presented him with detailed documentation and those who organized several meetings with him in order to provide detailed briefings.

5. Furthermore, the Special Rapporteur thanks those members of the Council of State and their staff who provided insights into issues of primary concern regarding privacy.

II. Constitutional and other legal protections of privacy

6. In France, privacy is considered to be a right protected by constitutional law. This despite the fact that there is no explicit written reference to the protection of private life in either the Constitution of 1958 or in the 1946 Constitution. Over the years, the right to privacy has, like a number of other rights,[3] been classified as a principle that has constitutional value, which, in French law, is the way of describing all those principles inferred by jurisprudence despite the fact that there may be no explicit reference in the written text of the Constitution. It is fair to say that the right to privacy in France has undergone a process of "constitutionalization" over the years, especially since 1977, when the Constitutional Council first took a major decision[4] on the subject. On 12 July 2018, the National Assembly refused to insert an explicit reference to privacy in the Constitution of France on the grounds that this right already existed and had been explicitly recognized in the jurisprudence of the Constitutional Council. This in spite of the recommendation made by a Senate commission in May 2009[5] and of the attempt made by Senator Anne-Marie Escoffier, also in 2009, to insert such a reference, an attempt that was rebuffed by the Ministry of Justice on 10 January 2010 for the same reasons subsequently advanced in 2018.

[1] Available from www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex4_Metrics_for_Privacy.pdf. The document was developed during the period 2017–2019 to enable the Special Rapporteur to maximize the number of common standards against which a country's performance could be measured. It has been refined in various stages and was released for public consultation in March 2019.

[2] See www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=22410&LangID=F (in French). The statement and the present report should be read together, especially since, for reasons of available space and editing, some observations, especially those about transitional measures like emergency laws, that were available in the 2017 text have been omitted from the present report.

[3] Including the respect for human dignity and the right to access public documents.

[4] Decision No. 76-75 of 12 January 1977.

[5] See www.senat.fr/rap/r08-441/r08-44148.html.

7. While, unlike in Germany, the Constitution of France makes no mention of the right to the free development of personality, French constitutional law encompasses an entire range of personality rights[6] with the freedom to develop them tracing back to article 2 the Declaration of the Rights of Man and of the Citizen of 1789.

8. Residents and citizens of France benefit from the protections set out in the General Data Protection Regulation,[7] which, however imperfect, is acknowledged as providing some of the highest levels of protection of privacy worldwide. The independent data protection authority of France (CNIL)[8] and certain measures and practices prima facie satisfy the requirements of the Regulation.

A. Legislation on surveillance

9. While the Special Rapporteur presented a draft legal instrument on government-led surveillance to the Human Rights Council in March 2018, and this may be used as an interim benchmark, there is as yet no universally agreed international binding multilateral treaty regulating such matters. Member States have therefore been very much left to "do their own thing" when it comes to safeguards and remedies in respect of State-led surveillance. The approach taken by France is very interesting, as it reflects a genuine concern to get to grips with the thorny problem of effective oversight of surveillance. France remains one of only some 13 States that have made serious attempts to address issues of adequate oversight of surveillance since the revelations made by Edward Snowden in 2013.

B. Surveillance

10. It is extremely important to note the following features and dynamics that have developed in the French system:

(a) Numerous debates on service reforms have recently taken place in the context of political and public media discussions. Unfortunately, the security situation in Europe has been difficult, with frequent attacks taking place since 2001. France has witnessed several attacks, in March 2012, in January and November 2015 and again in July 2016, with "lone wolf" attacks also persisting into 2020. The recurrence of these terrorist acts has led to an increased sense of threat;

(b) Since 2008, the French intelligence model has shifted from a dual model that distinguished the domestic from the foreign to a community model. Thus, in accordance with a white paper published in 2008 and Decree No. 2014-474 of 12 May 2014, the French intelligence community comprises six intelligence services (the General Directorate of External Security, the General Directorate for Internal Security,[9] the Directorate of Military Intelligence, the Defence Intelligence and Security Directorate, TRACFIN and the National Directorate of Intelligence and Customs Investigations), the National Coordinator and the Intelligence Academy. Decree No. 2017-1095 of 14 June 2017 adds the Inspectorate of Intelligence Services to the community. The six entities established in Decree No. 2014-474 are specialized intelligence services, a designation that distinguishes them from other services carrying out intelligence activities. Moreover, the specialized intelligence services have the right, to a certain extent, to request and carry out non-targeted surveillance,[10] whereas the non-specialized intelligence services (for example, the Intelligence Directorate

[6] See, e.g., Emmanuel Pierrat, "Protection des droits de la personnalité", *LEGICOM*, vol. 12, No. 2 (1996), pp. 87–93: "Dans son acception française, les droits de la personnalité recouvrent donc en vrac le secret de la correspondance et des conversations téléphoniques, le droit de s'opposer au traitement de données nominatives, les secrets de l'instruction et professionnels, le respect de la vie privée, le droit à l'image, le droit à la voix et le droit au nom."

[7] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[8] See www.cnil.fr/en/home.

[9] Formerly the Central Directorate of Internal Security.

[10] See Code of Internal Security, arts. L851-2 and L851-3.

of the Paris Police Department, the National Prison Intelligence Service and the Central Territorial Intelligence Service) can only carry out targeted surveillance as part of specialized intelligence missions;

(c) The Parliamentary Delegation on Intelligence was created by Law No. 2007-1443 of 9 October 2007, but responsibility was truly exercised only after the so-called military programming law came into force for the period 2014–2019. The General Secretariat for Defence and National Security announced in its 2018 report reforms to facilitate the exchange of information and simplify the procedure for declassifying documents;

(d) Control is not intended to be exercised directly on the intelligence services since they are primarily under the authority of the ministers concerned and then under the authority of the service directors. On the contrary, parliamentarians are associated with the proportionality control of intelligence techniques in the context not of the Parliamentary Delegation on Intelligence but of the National Commission for the Control of Intelligence Techniques, which is an independent administrative authority;

(e) The creation of a national intelligence council headed by a dedicated coordinator[11] with the mission to carry out joint inspections operating in a cross-cutting manner was discussed. The Inspectorate of Intelligence Services was then mentioned in the military programming law and finally created by Decree No. 2014-833 of 24 July 2014. It reports to the Prime Minister and carries out inspections on specialized intelligence services;

(f) Finally, Laws No. 2015-912 of 24 July 2015 and No. 2015-1556 of 30 November 2015 constitute a remarkable step forward for the oversight of intelligence services. They have led to the creation of administrative and jurisdictional controls on the use of intelligence techniques and files of interest for State security. The administrative control granted to two independent administrative authorities, the National Commission for the Control of Intelligence Techniques and CNIL, is a major step forward but does not constitute a conceptual rupture since it is in line with the traditional powers of CNIL on the one hand and of the entity that has been replaced by the National Commission for the Control of Intelligence Techniques on the other hand. The judicial control that is now exercised, on the basis of requests or complaints, by the competent independent administrative authority or individuals following a prior administrative check, marks a clear breakthrough. It is the first time that a judge is given access to classified documents without details being communicated to the applicant. These laws therefore constitute both a great step forward because of the unprecedented scope of administrative control they grant and a tangible evolution because of the creation of a mechanism for providing judicial remedies;

(g) During the 23-months-long state of emergency prior to October 2017, the practice of judicial courts (including the Council of State) has been to accept “white notes”. In order to justify police actions (house arrest, prohibition to demonstrate) against people suspected of challenging the State apparatus, the Ministry of the Interior frequently used white notes. The name comes from the fact that they are documents, attributed to the intelligence services, without heading, date, reference or signature. Aimed at protecting the secrecy of the sources, their anonymity also prevents anyone from having to take responsibility for the statements made on these notes. Experience has shown that the notes sometimes contained errors, such as references to convictions that had not been pronounced or to acts that did not actually exist. As long as we look at white notes as “evidence”, it is very difficult to distinguish, in practice, the value of these anonymous documents drawn up without any guarantee from that of the records that the law strongly oversees. Since the new law on terrorism of November 2017 does not mention them, it will be interesting to follow how the judicial courts will see these white notes going forward, in other words whether the notes will be considered as evidence or given some other value.

[11] See Decree No. 2009-1657 of 24 December 2009.

C. Surveillance for the purpose of law enforcement

11. In France, surveillance prerogatives differ according to purpose: the specialized intelligence services have as their main and final goal the assurance of national security, whereas the police and sometimes the gendarmerie (a paramilitary force) focus on ensuring public order.

12. On French territory, communications interception is authorized under two distinct frameworks:

(a) Judicial interceptions ordered by a judge of inquiry during a criminal investigation. Such interceptions can be done by the police, the gendarmerie and the General Directorate for Internal Security;

(b) Administrative interceptions, also known as security interceptions, requested by both the domestic security and foreign intelligence services.

13. Moreover, French law provides for investigative judges to order the interception, recording and transcription of private telecommunications in criminal investigations and law enforcement authorities may obtain authorization to ask any qualified person to perform the technical operations that would allow access to this information.

14. The National Assembly set up a parliamentary committee in January 2016 to examine the attacks on the offices of the satirical newspaper *Charlie Hebdo* and elsewhere in the Paris area in January 2015 and also to examine a coordinated series of assaults by Islamic State in and around the French capital in November 2015. A total of 147 people were killed in those attacks. The parliamentary committee did not directly criticize the Government's response to the attacks, although it raised questions about the efficacy of the state of emergency declared in November 2015 and of the deployment of 10,000 soldiers around the country to protect cities and other sensitive areas. In its report, the parliamentary committee revealed that the National Police, which is charged with protecting large cities, and the gendarmerie, which is charged with protecting small towns and rural areas, have separate intelligence divisions, which should be merged.

15. Law No. 2017-1510 of 30 October 2017, which was passed by a large majority and ended the state of emergency, has strengthened the powers of the executive (e.g. prefects) to assign someone to carry out house searches, close places of worship where ideas for terrorism are disseminated or carry out identity checks near borders and at railway stations, seaports and airports, all without first getting the judicial green light (with the exception of searches). Prefects' decisions to have houses searched and people confined are still based on very shaky legal grounds, for example, on informal, anonymous and often vague notes by the secret services. For persons who contest a search, there exists an appeal procedure. Civil rights campaigners claim that Law No. 2017-1510 places citizens under a general blanket of suspicion. These security parameters invert an important principle of French law, and the police no longer needs a reason to search. Civil society representatives have also underscored that the principle that "everybody is a suspect and if you have nothing to feel guilty about, you won't mind the police frisking you" is not a prerogative of the respect of human rights, quite the opposite.

16. The provision concerning wireless tapping, which was censured in October 2016 by the Constitutional Council, has been reintroduced. The law now clarifies the legal framework for using it, as no controls had been planned before. The text also extends until 2020 the decried concept of black boxes for intelligence, which use algorithms to detect suspicious connections on the Internet.

17. Other security measures have been incorporated into ordinary law by Law No. 2017-1510. Among them is the creation of passenger name records, which allow the authorities to access the names of all passengers on commercial flights in Europe and for the investigation of members of the public who may have become radicalized.

D. Surveillance for the purpose of national security (domestic and foreign surveillance)

18. Administrative interceptions are approved by the Prime Minister. In France, the national intelligence and security services must obtain prior authorization from the Prime Minister or his or her delegate, upon the written request of a senior minister, to intercept and read private communications for specifically enumerated purposes, and may request from providers of cryptology services the means to decipher encrypted communications.

19. The main French security and intelligence services are the following:

(a) The General Directorate for Internal Security, which reports to the Ministry of the Interior and is responsible for domestic security. It has some 3,500 employees and an annual budget of 300 million euros. The General Directorate for Internal Security was formed in 2008 through the merger of the Central Directorate of General Intelligence and the Directorate of Territorial Surveillance of the National Police;

(b) The General Directorate of External Security, which reports to the Minister of Defence and is responsible for collecting foreign intelligence on civilian issues and also performs paramilitary and counterintelligence operations abroad. The General Directorate of External Security is responsible for both human and signals intelligence. It is a foreign intelligence service that is not supposed to operate on French territory but is authorized to request data and intercept domestic communications. Moreover, it has the most technical capabilities for decryption and high-end communications collection and provides other agencies, such as the General Directorate for Internal Security and the Directorate of Military Intelligence, with technical means and expertise;

(c) The Directorate of Military Intelligence, which reports directly to the Chief of Staff and to the President of France as the supreme commander of the French military. It is part of the Ministry of Defence. The Directorate of Military Intelligence is responsible for collecting military intelligence in support of the French armed forces;

(d) The Defence Intelligence and Security Directorate (part of the Ministry of Defence) is responsible for the security of information, personnel, material and facilities of the armed forces and of the defence industry;

(e) The National Directorate of Intelligence and Customs Investigations, which is part of the Ministry of the Economy and focuses on foreign intelligence consisting of border issues;

(f) TRACFIN, which is a unit of the Ministry of the Economy and has intelligence-gathering capabilities, especially concerning money-laundering and the financing of terrorism. It focuses on foreign intelligence.

20. Decree No. 2015-1639 of 11 December 2015 granted authority to more than 20 police and gendarmerie services, some of which are not officially intelligence services, to intercept communications and request data, mostly for counter-terrorism purposes. Allowing police services to collect communications intelligence represents a shift from older French habits, which the Government of France views as justified given the ongoing terrorist threat.

21. As in most countries, in France the law provides greater privacy protection to its own citizens and people communicating from France than to people communicating from abroad, who, at law, receive little legal protection against intelligence collection. Intelligence collection activities approved by the Prime Minister may be carried out in respect of all electronic means of communication traced to a targeted individual, including those involving mobile and landline telephones, all metadata from Internet service providers and other online services.

22. In France, telephone companies, Internet service providers and providers of online services can be compelled to provide a wide range of metadata regarding a targeted user, including technical data related to the identification of connection or subscription numbers (telephone numbers, IP addresses etc.), a list of all connection or subscription numbers linked to a targeted individual, location data of all devices traced to a targeted individual and call detail records. With the Prime Minister’s approval, telephone companies can be compelled

to cooperate with intelligence services conducting targeted telephone call interceptions. French intelligence services are not supposed to proceed with conducting interceptions on their own but have to go through a dedicated government technical agency called the Interministerial Control Group.

23. Parliament has authorized the intelligence services to use devices such as international mobile subscriber identity-catchers (IMSI-catchers) to identify and locate mobile telephones or computers linked to targeted individuals. The intelligence services can only use IMSI-catchers to collect metadata, and all collected data unrelated to specified targets must be destroyed. The law on intelligence presented to the Council of Ministers on 19 March 2015 goes further in the logic of weakening judicial control, formally allowing the intelligence services to carry out a number of previously illegal practices and technologies, including IMSI-catchers, geolocalization of cars, the wiretapping of private places and vehicles, the granting of access to networks of private Internet service providers and the placement of black boxes[12] on networks in order to guess the identity of suspected terrorists through the use of algorithms. None of these require judicial authorization. There is a possibility for an a posteriori control[13] – a measure that can be considered too weak as a guarantee for human rights, privacy and democracy given the scope of intrusion. The use of black boxes represents the most massive surveillance system deployed by the intelligence services on the communications of French citizens. In October 2017, the National Commission for the Control of Intelligence Techniques gave a favourable opinion on the deployment of the first such algorithm for the purpose of preventing terrorism. First, algorithm has to be approved by the Prime Minister on the basis of a positive opinion of the National Commission for the Control of Intelligence Techniques and assurances that, once the algorithm has been deployed, it only works with anonymized data (only connection data, not content data). Second, when the algorithm notifies that it has found data that deserve special attention, the service that requested the activation of the algorithm can request that the data be deanonymized. A new approval from the Prime Minister and a new opinion of the National Commission for the Control of Intelligence Techniques are needed in order for the deanonymization to take place. Third, after the deanonymization of the data, the intelligence service may request that other classic surveillance techniques be deployed on the targeted person.

24. French telecommunications and Internet service providers are already compelled by law to store their customers' metadata for at least one year. Moreover, a French legal decree even requires website-hosting companies like Facebook, Google and Amazon to store their user data for at least one year and provide them to government authorities at their request. However, these metadata may be used only for targeted investigations, as the intelligence services must go through a full process that requires the provision of specific requests to Internet service providers and website-hosting companies with either the full name of a target, its user name, IP address or other identifying information and the approval of the Prime Minister. It seems that installing black boxes on the networks of Internet service providers serves to also facilitate the bulk collection of smaller sets of data. Black boxes filter traffic using specific threat-detection algorithms, so they will likely pull in only those metadata which match certain selectors, including communication patterns and routines, based on digital forensics from counter-terrorism investigations. The metadata would then be used to identify the users showing such patterns.

25. Regarding domestic communications, voice communication recordings must be destroyed 30 days after collection, but transcripts can be kept for "as long as necessary" by intelligence services. Metadata requested from Internet and telecommunications service providers can be stored for up to four years. Intercepted communications that are encrypted can be stored for up to six years.

26. The Ministry of the Interior has underlined the fact that current laws force the intelligence services to employ only targeted surveillance, with the exception of algorithms, in which case pseudonymization must be used.

[12] See Law No. 2015-912 of 24 July 2015, art. 5, and Code of Internal Security, art. L851-3.

[13] If the Prime Minister does not follow the opinion of the National Commission for the Control of Intelligence Techniques, the latter can submit an appeal to the Council of State.

27. Two laws concerning terrorism and security have been adopted: the military programming law for the period 2014–2019, in December 2013, and the "anti-terror law", in November 2014. The first provides a framework for the use of real-time geolocalization by intelligence services. The second allows administrative blocking of websites considered as condoning violent acts of terrorism.

28. Fewer restrictions apply to the surveillance of foreign communications, whether by the General Directorate for Internal Security, the General Directorate of External Security or one of the military agencies. After having received the opinion of the National Commission for the Control of Intelligence Techniques, the Prime Minister issues broad-ranging authorizations to intelligence services that allow them to monitor and collect communications data, either for whole geographical regions, countries, organizations or individuals. The Prime Minister specifies which types of communication networks can be targeted for collection. These authorizations last four months but can be renewed without restriction.

29. Foreign intercepted communications data can be kept for one year after processing or for up to four years after collection. Collected metadata can be stored for six years. Encrypted data can be stored for up to six years after decryption or for up to eight years after it has been collected.

30. The law on the surveillance of foreign communications only applies to communications between users who are outside of France, but which are collected from within French territory, including overseas territories, especially as this is stated in the latest intelligence laws. This means that the law applies not only to data collected from major fibre-optic cables and satellite intercept stations inside France, but also to those from such overseas satellite stations as those in French Guiana, New Caledonia and Mayotte, thereby providing the French intelligence community with a global satellite communications coverage probably second only to that of the Five Eyes partnership between Australia, Canada, New Zealand, the United Kingdom of Great Britain and Northern Ireland and the United States of America, which gave rise to the Echelon surveillance programme. The French signal intelligence network has been dubbed Frenchelon, in reference to that programme. If data are collected under the foreign communications status, but are subsequently traced back to domestic communications (the call number or the subscription are located in France), they can be processed only if approved under the domestic communications framework or must be destroyed within six months.

31. Since 2008, the General Directorate of External Security has been able to connect directly to underwater cables to intercept Internet traffic therein. Surveillance has shifted from targeted to massive.

32. The Ministry of the Interior has explained that, pursuant to the Code of Internal Security, an intelligence service can only employ one specific technique for one specific purpose or finality (see art. L801-1 of the Code).

33. The Ministry of the Interior has confirmed a prior statement of the National Commission for the Control of Intelligence Techniques indicating that, in France, the intelligence services do not engage in bulk/mass surveillance.

E. Oversight of agencies carrying out surveillance

34. Laws such as Law No. 2015-912 and Law No. 2015-1556 grant the Prime Minister full authority to order and approve both domestic and foreign intelligence activities. Each request for data collection is sent by the intelligence service director to its parent ministry and to the Prime Minister, who gives final approval. Such ex ante control focuses on proportionality, legality and subsidiarity (i.e., on checking whether other, less intrusive, techniques are available).

35. The new law of November 2017, which also requires that the National Assembly and the Senate be kept informed by the administrations, which will in turn transmit a copy of all acts taken, is valid only until 31 December 2020.

36. For oversight purposes, the National Commission for the Control of Intelligence Techniques is kept informed of all requests and supervises the implementation of intelligence techniques.

37. The National Commission for the Control of Intelligence Techniques plays only an advisory role and cannot overrule any decision by the Prime Minister regarding requests for intelligence data collection. The National Commission can express disapproval of a collection request, but the Prime Minister can overrule its advice and authorize intelligence collection. The National Commission can notify the Council of State if the Prime Minister does not respect its advice.

38. The National Commission for the Control of Intelligence Techniques can access all transcripts and logs from intelligence collected with the Prime Minister's approval but cannot compel any intelligence service to produce other documents or information, nor can it investigate any irregularity on its own initiative. All a posteriori controls take into consideration the existence of prior authorization and how the techniques were implemented. The National Committee can, however, make recommendations regarding intelligence procedures, notify the Prime Minister about any irregularities found and bring any irregularity to the attention of the Council of State. All debates held in the framework of the National Commission, as well as all its communications with the Prime Minister and intelligence services, are classified.

39. In some special cases (such as breaking and entering) it is mandatory for the National Commission for the Control of Intelligence Techniques to notify the Council of State. In the rest of the cases, such notification is not mandatory but, rather, at the National Commission's discretion. The notification does not have a suspending effect but the Council of State can issue a judgment expeditiously (i.e., in less than one day).

40. Special status has been granted to journalists, lawyers and members of parliament. When an intelligence request is made that applies to them, the National Commission for the Control of Intelligence Techniques must be informed just before data starts being collected so that it can assess whether the collection is necessary and proportionate. The National Commission must also receive transcripts of the intercepted communications afterwards. The difference with regard to eavesdropping operations against regular citizens is that, for them, the National Commission can access the transcripts if it asks for them, while it must receive and review the transcripts involving members of privileged professions.

41. In theory, any individual living in France or abroad can ask the National Commission for the Control of Intelligence Techniques to check if he or she has been placed under surveillance following proper procedure. The National Commission must then check for any irregularities but can neither confirm nor deny to the individual that he or she has been placed under surveillance. The National Commission can only state that proper verification has been made and report any irregularity that it has detected to the Council of State.

42. The main issue concerning the powers of the National Commission for the Control of Intelligence Techniques is their ex ante control.

43. Another interesting enrichment of the powers of the National Commission for the Control of Intelligence Techniques was brought by Law No. 2017-1510, which gives the National Commission control over the interception of wireless communications, and the decision of the Constitutional Council of 21 October 2016.

44. The 2017 report of the National Commission for the Control of Intelligence Techniques brings to surface some interesting figures, especially concerning the number of requests made for approving the use of certain surveillance methods. Specifically, 70,432 opinions were issued by the National Commission in 2017, 5 per cent more than in 2016. Of that total, 30,116 opinions concerned requests of identification of telephone subscriptions or telephone numbers, according to the president of the National Commission the most used of the less intrusive techniques in France. A significant number of opinions (8,758, 5 per cent more than in 2016) concerned requests for security interceptions. Access to detailed telephone invoices was requested 18,512 times in 2017.

45. The greatest increase in the number of requests has been noted in those concerning real-time geolocalization, which rose by 55 per cent compared to 2016.

46. The percentage of a priori negative opinions (3.6 per cent in 2017 compared to 6.9 per cent in 2016) shows that the intelligence services are improving their understanding of what they are allowed to do under the law and of how to ask for it. The Prime Minister did not use the emergency procedure in either 2016 or 2017; the only time he did so was at the end of 2015, in the face of a suspicion of an imminent terrorist attack. On the other hand, more than 21,000 persons have been put under some kind of surveillance at least once, without any judicial inquiry having been opened as at the time of publishing the 2017 report. Of that total, 42.8 per cent (9,157 persons) were put under surveillance for the purpose of preventing terrorist acts, 5 per cent more than in 2016. The other purposes for approving surveillance techniques have been: prevention of crime, including organized crime (18 per cent), protection of major foreign policy interests (17 per cent), protection of the interests of France (8 per cent) and prevention of activities destabilizing the public order (6 per cent).

47. In 2017, the National Commission for the Control of Intelligence Techniques carried out 130 a posteriori controls (compared to 60 in 2016). As no major problems were noticed, it appears that no attempt was made by the intelligence services to eschew the law.

48. CNIL is the regulator of personal data. It assists professionals in their compliance and helps individuals to control their personal data and exercise their rights.

49. CNIL does not, however, have access to or exercise public control over intelligence files beyond knowing of their existence.

50. CNIL underlines that the new antiterrorist law (Law No. 2017-1510) may represent the paradigm of surveillance. In the past, the authority would identify dangerous persons and then put them under surveillance. Now, it puts everybody under surveillance in order to identify those who represent a threat. It is unclear what the status of black box surveillance is given the recent decisions of the European Court of Justice, although it could be argued that the existence of selectors makes it a form of targeted surveillance and that pseudonymization is an adequate safeguard.

51. CNIL also raised the issue of the training of judges and whether judges should have technical expertise.

52. A specialized task force responsible for addressing disputes arising from the deployment of surveillance techniques for protecting the security of the State and for addressing disputes relating to indirect access to a document was created in November 2015 and is part of the Council of State. It can be notified by citizens only after referral to other authorities. They first ask CNIL to carry out an audit. The National Commission for the Control of Intelligence Techniques must be notified as well. Only after all these steps have been taken can individuals take the complaint to the specialized task force. The members of the task force (five State councillors and two special rapporteurs) have access to defence secrets. The judges can ask anything and have access to everything, while complainants cannot, a sign of asymmetrical contradictory application: the judges have all the power and the administration must answer all questions asked; complainants, on the other hand, cannot be informed of the answers provided. A certain balance and trust between the powers of the State are therefore assured.

53. When the National Commission for the Control of Intelligence Techniques gives a negative opinion and the Prime Minister does not respect it, the National Commission can submit a complaint to the specialized task force of the Council of State and ask for the dispute to be resolved through arbitration. During the two years prior to November 2017, the Prime Minister never ignored a negative opinion of the National Commission.

54. The work of the specialized task force was initially impeded by its inheritance of over 100 cases from the Paris courts. Currently, only around 10 cases per year focus on surveillance complaints. Currently the focus is on the files, namely the erasure of data that had been irregularly harvested. Regarding cases involving the surveillance of foreigners, complaints arise because those interested in carrying out the surveillance chase more in-depth checks.

55. Regarding the composition of the various oversight agencies, the members of the National Commission for the Control of Intelligence Techniques have technical expertise in information and communications technologies. The president of the specialized task force

has highlighted that the task force's members, who have legal expertise, lack such specialized expertise in information and communications technologies and would therefore benefit from technical training or a manual to guide them further.

56. The Council of State also has consultative powers regarding the adoption of a law, its opinion being mandatory in what concerns the legality and conformity of the new law. Although this kind of ex ante control is of a specialized nature, the members of the Council of State who enjoy judicial status and who analyse new proposed laws do not have technical knowledge. They have indicated that it would not be appropriate to have some independent experts as part of the team, preferring instead having the administration take the decision with the help of experts, thereby assuring accountability. Should an external organ conduct controls and take decisions, there would be the risk of the Council of State being bypassed.

57. The Councillors of State also expressed concern that a law had been drafted for a system of protection for simple interceptions but that no one appeared to have thought about all the metadata with a more detailed profile of an individual. This aspect must be studied together.

F. Health data

58. Law No. 78-17 of 6 January 1978, which has been amended several times and been largely supplanted by the General Data Protection Regulation, is essential for protecting personal health-related data, namely data that allows for the identification of persons, while it underlines the principles of lawfulness, limitation by purpose, conservation for a limited period and the importance of ensuring that data are accurate and up to date.

59. Law No. 2016-41 of 26 January 2016 made important alterations to the above-mentioned text. It is articulated around three objectives: reinforcing preventive medicine, reorganizing access to localized health care by general practitioners and strengthening respect for the rights of patients. It also uncovered the existence of pseudonymized data. Another essential aspect is its insistence that any organ wishing to have access to data must demonstrate that obtaining such data is in the public interest. This is a promising practice applied by France that is not often applied elsewhere in Europe and that represents a necessary safeguard for protecting patients' privacy. The obligation to demonstrate public interest allows for exceptions, such as marketing, the promotion or exclusion of health benefits and insurance. The main guarantee is provided by CNIL, whose authorization is mandatory. The law also includes an obligation to respect the principle of transparency; in practical terms, this means that when medical data are used for medical research, the results of medical research, the results of the research must be made public.

60. Health data are considered sensitive data and should be treated as such. The role of CNIL appears in cases of exceptions to the rule, such as public interest. Moreover, CNIL must consider the question of consent and the principle of access to information, as well as patients' rights, when it analyses one of the exceptions.

61. The National Institute of Health Data offers opinions on data processing to CNIL.

62. Concerning the authorization to handle medical data, the data hosts must be certified in security management and risk analysis. It is prohibited for data holders to share medical data for financial gain, even with consent.

63. France applies the principle of open data but also focuses on preserving the data. In other words, data cannot be reused for another purpose (except for statistics). In France, open data are strictly anonymous.

64. Regarding modern technologies, including wearable fitness trackers, the main problem is that a simple one-click consent is not enough of a safeguard, since most people do not understand what their consent entails or to what they are really consenting. Therefore, another solution must urgently be found to the constant rise in the number of technologically interconnected devices, digital transformations, including in the medical field, which unveil more vulnerability and potential risks of attack.

65. CNIL has noted that anonymized open data fall beyond its scope of action. Many private actors want to have access to such data, which must be collected transparently, and this is where CNIL intervenes: by informing individuals that they can oppose the publicization of their data and by requiring that publicly available data must be perfectly anonymized, not pseudonymized.

66. There is also the requirement to maintain the confidentiality of health data, for example, through the digital hospital programme for 2012–2017. It appears that, late in 2017, some 2,000 of 3,000 health facilities were in compliance with the confidentiality requirement. The current aim is to increase the requirements and the number of compliant establishments, notably by meeting the requirements set out in the HOP'EN programme (2019–2023), a strategic plan of action for hospital information technology systems that follows on from a previous programme also aimed at developing the information technology capacities of hospitals (*hôpital numérique* programme).

67. CNIL engages in a productive dialogue and in consultations with hospitals but has underlined the fact that the budget is often insufficient in special conditions.

III. Conclusions and recommendations

A. Intelligence oversight, security and surveillance

68. **For the past 300 years, the discussion about forms of government has consistently paid attention to the checks and balances that may exist between the three branches of government: the executive, the legislature and the judiciary. Considerations about surveillance in any given society therefore have to take into account the checks and balances which may be incorporated and those which have been omitted from the system. When one surveys the various forms of authorization of surveillance around the world, the following categories may be identified:**

(a) **Exclusively internal to the service (by "service" one meaning both security services such as an intelligence service or a law enforcement agency primarily tasked with public order and the detection, prevention and investigation of crimes and the prosecution of those responsible);**

(b) **External to the service, exclusively given by a politician occupying an executive position, normally a ministerial post, sometimes even that of Prime Minister;**

(c) **External to the service, exclusively given by one or more members of the judiciary, with absolutely no involvement of any politicians at any stage of the process;**

(d) **External to the service, given by a hybrid system, where the first authorization is given by a politician that is then reviewed by one or more members of the judiciary, the so-called double-lock system.**

69. **It is understandable that a country's elected government, consisting largely or exclusively of politicians, would identify priorities in matters of foreign policy and thus reasonably set some policy priorities for its intelligence services would then have to operationalize. These generic directions in matters of foreign intelligence would understandably include issues with allies and hostile countries, negotiating and trading partners, whom to assist, whom to be wary of and whom to be careful not to offend. The situation is quite different when matters of national security relate to the activities of domestic intelligence services, which should have sufficient guidance from the Constitution they are normally tasked to protect and from the detailed provisions of national laws aimed at ensuring that fundamental human rights are adequately protected.**

70. **When it comes to privacy, the metric is clear: privacy cannot be infringed except for certain specific purposes, such as national security and the detection, prevention and investigation of crimes and the prosecution of those responsible. Even in those instances, the interference with privacy is only permitted by measures that are provided for by law and that are necessary and proportionate in a democratic society,**

irrespective of whether it is a matter of foreign or domestic intelligence. The checks and balances that kick in should be equally clear: the politicians in the legislative branch of Government, in most democracies, led by the politicians controlling the executive branch, formulate and approve the provisions of the law that serve as safeguards and remedies in the case of privacy. Action is taken within the strict parameters of the law by security services and law enforcement agencies, which normally answer to members of the executive. The legality of their actions is then decided upon by the judiciary.

71. **An additional part of the system of checks and balances is carried out by the legislature through parliamentary committees tasked with oversight of the security services. In most cases, however valuable, this can only be a high-level form of ex post oversight, restricted largely to correct execution of policies and utilization of fiscal resources approved by the legislature since such committees lack the time, resources and expertise required to carry out detailed scrutiny of operations.**

72. **There is no clear, let alone overwhelming, evidence that politicians of any sort, whether members of the executive or of the legislature, add any value to day-to-day decisions about who, should be put under surveillance, or about when and how they should be put under surveillance especially in matters of domestic intelligence. On the contrary, history is replete with examples of politicians in power using domestic intelligence abusively in order to cling to power. As a rule, therefore, the involvement of politicians in ad hoc decisions about whose telephone line should be tapped, whose smartphone should be infected with malware, whose office or bedroom should be bugged and when and why any of the above should occur should be avoided to the greatest extent possible. Yet, in the pre-democratic past of most countries, the direction and control of spies was part of the prerogative of the all-powerful executive. This is a part of history that many democracies have not yet managed to shake off. Despite the fact that there is no evidence that they add any value to the process, there remain several vibrant democracies where the ad hoc decisions about who to spy on are taken on a daily basis by members of the executive.**

73. **The best practices adopted globally suggest the following:**

(a) **Intelligence and police officers at all levels should be given comprehensive training on human rights, with a special focus on which conduct and measures are necessary and proportionate in a democratic society;**

(b) **Every time that an intelligence or police officer wishes to carry out any form of surveillance, he or she must be obliged by law to justify how said surveillance is provided for by law and how it meets the tests of necessity and proportionality and attach those considerations at each and every stage of internal authorization within a service;**

(c) **Every time a senior officer within an intelligence service or a law enforcement agency is required to approve operations requiring any form of surveillance, he or she should be required to check the legal basis and the justification of necessity and proportionality and then, by law, he or she should be required to refuse to approve a surveillance operation if the correct legal basis is not present or if the tests of necessity and proportionality have not been adequately met;**

(d) **Subject to consistent and multiple applications of tests of legality, necessity and proportionality within the service, the first decisions about who should be placed under surveillance, and when and why, are normally best left to those professionals within the services with a detailed knowledge of current risks and actors. These internally validated decisions should, however, always be subject to authorization by a truly independent external entity or individual. An overzealous or abusive service may need to be kept in check, but politicians are often not best placed to act as an adequate check;**

(e) **In some countries, external authorization has traditionally been given by a judge who sometimes has minimal or no training in how an intelligence service or law enforcement agency really works. While working reasonably well in some instances, this practice has led to an enormous variation in the quality of decisions made about**

surveillance: in some countries, some or many judges are excellent and provide robust challenges to the services requesting authorization for surveillance, while in other countries they simply nod things through. In yet other countries, the very independence of the judges has been questioned, and consequently their ability to truly stand up to requests from the executive to carry out surveillance is likewise questionable, especially if they depend on the same executive for reappointment to their posts. In other countries, the external entity is often only external to the service but not external to the executive and is often a leading member of the executive such as ministers or Prime Ministers;

(f) **Some countries, like the Netherlands and the United Kingdom, have, since 2015, like France developed truly independent expert authorities that combine several areas of domain expertise (legal, operational and technical) but that, also like France, retain the involvement of politicians at some point or another in decision-making about surveillance. It is respectfully submitted that the quality of the decision-making about surveillance would not suffer at all if the external authorization were:**

(i) **In cases of domestic intelligence, restricted to the independent expert body alone;**

(ii) **In cases of foreign intelligence, restricted to the independent expert body, which should, however, take into account any opinions expressed on the matter by the Minister of Foreign Affairs.**

74. **France sets a good example internationally by creating, by law, a strong independent agency or expert authority responsible for oversight of surveillance: the National Commission for the Control of Intelligence Techniques. France, like Germany, the Netherlands and the United Kingdom, to name three European States, and Canada and the United States, to name two North American States, has dedicated considerable thought, effort and legislative time to creating one or more independent[14] oversight agencies tasked with reviewing all the activities of national security and intelligence agencies. This is a good practice that the Special Rapporteur strongly recommends all Member States to take up. In this respect, France also complies with its international obligations by following the spirit and the letter of article 9 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and article 11 of that Convention as amended by creating a law that provides safeguards, of which an independent oversight agency is one of the most significant.**

75. **As seen in the section on surveillance above, it is a feature of the French legal system to include politicians in the process required for prior (ex ante) authorization of surveillance, with the independent oversight body carrying out a review of that executive decision. Given the involvement of the National Commission for the Control of Intelligence Techniques since 2015, it could be said that the system of oversight of surveillance in France is a hybrid one,[15] with the request being subject to review by the independent oversight body (the National Commission for the Control of Intelligence Techniques) before the decision being taken by a politician (the Prime Minister). France is not the only democracy that continues to opt for this approach, which is nonetheless one redolent of a power carried over from earlier days, when the executive was sovereign and supreme, unchallenged in its power. It is also a power that consistently makes politicians and civil society representatives in many countries uncomfortable, with a quasi-perennial fear voiced to the Special Rapporteur in many countries about the risk of abuse of such power by the executive of the day. It is not, therefore, a system that the Special Rapporteur would especially single out as a good practice to follow. While no evidence has come to light of abuse of such power by the Prime Ministers of**

[14] Some are more independent than others. See the report of the Special Rapporteur on his visit to the United States in 2017, to be submitted to the Human Rights Council at its forty-sixth session, and subsequent correspondence to that country's Government in July 2020 lamenting the structure of United States law permitting the dismissal of the United States Inspector General of Intelligence at the sole discretion of the President of the United States, a factor which may detract from the independence and effectiveness of the office.

[15] Except in cases where surveillance is ordered by an investigating judge or magistrate.

France since the latest legal reforms of 2015, it would be preferable if the next round of reforms in France would alter the mechanism in such a way as to ensure that the ex ante authorization of surveillance is carried out by a completely independent entity, with no politician involved in the process. If nothing else, in this respect, France would be setting a good example to the rest of the world, where one finds an abundance of abusive politicians clinging to power.

76. **The system of oversight of intelligence in France cannot be described as being broken, not by any stretch of the imagination. On the contrary, it is one which is relatively strong and which appears to work well in practice. The current role of the National Commission for the Control of Intelligence Techniques is, however, by law, purely an advisory one and, especially if involvement in the decision-making process by a politician is retained for any length of time, the power to revoke a decision about surveillance should be entrenched in law, as should the good practices outlined in paragraph 73 (a)–(c) above. At a minimum, the National Commission should have the power to overrule and revoke any authorization for surveillance signed off by the Prime Minister, who, very preferably, should never be involved in such decisions.**

77. **During further consultations held after the visit, some cited French constitutional law and practice as providing the grounds on which to retain involvement in authorization of surveillance by the executive. This notwithstanding, France has contributed much to the theoretical foundations of the separation of powers in government and perhaps the time has come for France to again pioneer new thinking, 300 years into national and global testing of variations of the ideas of Montesquieu, Voltaire and Rousseau. Given that the *philosophes* had no idea of the complexities introduced by modern technologies with consequences, including much domain expertise, France should seriously consider leading the next refinement of the doctrine of the separation of powers with the creation or consolidation of a separate, independent hybrid entity. Whether such an entity should be independent from the National Commission for the Control of Intelligence Techniques and be responsible exclusively for ex ante authorization is also something to be considered. Alternatively, whether the status of the National Commission should be further elevated so that its decisions on surveillance, both ex post and ex ante, are absolute should also be considered.**[16] **The most important thing is that this separate, independent authority would combine adequate resources mastering several areas of domain expertise (legal, operational and technical), possibly with the continued contribution of senior judges, and that it should be empowered to authorize and/or monitor surveillance through decisions made completely independently and often even without the knowledge of the politicians forming part of the executive.**

78. **The Special Rapporteur has noted with satisfaction the practice adopted by the National Commission for the Control of Intelligence Techniques, at the request of the Government of France, of applying to foreign surveillance the same regime of safeguards as is applied for domestic surveillance activities. This in spite of the fact that, strictly speaking, the law applicable to foreign intelligence (Law No. 2015-1556 of 30 November 2015) is not as stringent on such matters as the law on domestic intelligence (Law No. 2015-912 of July 2015). In the light of the success of this experiment, and in compliance with the principles of international law, the Special Rapporteur observes that this is a situation where de facto should become de jure. He very strongly recommends that the next round of reforms of French law on the matter should bring the system of safeguards and remedies applicable to foreign intelligence in line with those required for domestic intelligence. This is consistent with the Special Rapporteur's recommendation to the Human Rights Council that the right to privacy**

[16] The Investigatory Powers Commissioner's Office of the United Kingdom has been vested with the power to make both ex ante and ex post decisions in all cases of surveillance, irrespective of whether the surveillance is carried out by an intelligence service or a law enforcement agency. As the Special Rapporteur notes in the report on his visit to the United Kingdom (to be submitted to the Human Rights Council at its forty-sixth session), that Office seems to have developed into a very effective oversight body and there has been resistance to comments made that, by dealing with surveillance both ex ante and ex post, it could be accused of "marking its own homework".

should not depend on the passport in one's pocket. A person's privacy should be protected irrespective of one's physical location.[17] This measure too would help France to set a good example internationally, joining Germany, whose Constitutional Court compelled the Government of that country, in May 2020, to amend the law governing foreign intelligence to take it in a more equitable direction, one protective of human rights.

79. **An excellent practice entrenched in French law since the reforms of 2015 is the unlimited access of the National Commission for the Control of Intelligence Techniques to logs and data collected through activities authorized by the Prime Minister. The Special Rapporteur recommends that this practice be extended to all the files and records of the intelligence services. This is an essential power that all Member States should emulate and would be a good example set by French legislation for other Member States to follow. It is useless to create an oversight agency without also giving it the legal power and the adequate resources to do its job properly and full access to the paper and computer systems of the intelligence services and the law enforcement agencies.**

80. **Another excellent practice developed by the National Commission for the Control of Intelligence Techniques is that of maintaining within its structures – and deploying – technical expertise. By examining and testing, before operational deployment, the source codes for algorithms used for analysing metadata in communications, the National Commission has provided an additional safeguard prima facie implementing the principles of targeted surveillance required by the European Court of Human Rights and the European Court of Justice.**

81. **Furthermore, the Special Rapporteur notes with approval the additional safeguard that, should an automated analysis of metadata flag an interesting set of transactions or users, then the intelligence service concerned is required to request authorization of the oversight agency, the National Commission for the Control of Intelligence Techniques, in order to access any relevant databases.**

82. **The Special Rapporteur has noted with satisfaction the important developments regarding remedies for citizens in administrative litigation. In effect, the creation of a special team of five judges of the Council of State each empowered to have full access to the files of the intelligence services is an important remedy established since 2015 for those citizens seeking remedies for the illegal collection of information about them.**

83. **Following discussions with judges and representatives of CNIL and the National Consultative Commission on Human Rights, the Special Rapporteur very strongly recommends that all persons with legal training involved in the oversight of surveillance should also be given adequate training in information and communications technologies and operational best practices.**

B. Modernizing the data protection law of France

84. **A State member of the European Union, France has recently completed its second year of implementation of the General Data Protection Regulation. As the Regulation has a built-in review mechanism, it is expected that the Government of France will, together with all relevant agencies and ministries, be contributing to the review process held at the European Union level.**

C. Privacy and health-related data

85. **The coronavirus disease (COVID-19) pandemic has provided an opportunity for reflection, also about the detailed enforcement of those provisions of the General Data Protection Regulation regarding health-related data. Most, if not all, of the issues raised**

[17] Except in instances such as imprisonment where additional surveillance may be authorized by law in line with clearly prescribed modalities.

by the computerization of health records, the related use of artificial intelligence, technology applications in contact-tracing and standards to be respected, even in a pandemic, have been addressed by the Special Rapporteur in recommendations on the subject[18] and an accompanying explanatory memorandum.[19] The Special Rapporteur therefore respectfully draws the attention of the Government of France to the recommendations on the protection of health data contained in his report submitted to the General Assembly in August 2019.[20] These recommendations, in some instances, go further than, although they are completely aligned with, the principles set out in the General Data Protection Regulation and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as amended. The Special Rapporteur urges the Government of France to reflect on the successes – and the failures – in attempts to use applied technologies and especially smartphone applications in its attempts to fight the COVID-19 pandemic.

D. Gender and privacy

86. **During his visit, the Special Rapporteur observed instances when gender could have an impact on how privacy was experienced. He therefore respectfully draws the attention of the Government of France to the findings and recommendations on gender and privacy contained in his report submitted to the Human Rights Council in March 2020.[21] The principles outlined therein should be closely respected and implemented in any forthcoming reform and in any contribution made by France to the debate on reviewing and reforming applicable data protection laws, including the General Data Protection Regulation.**

E. Big data analytics, open data, children and privacy

87. **During an event supported by the United Nations Children's Fund (UNICEF) and held in Paris six months prior to his official visit to France, the Special Rapporteur appreciated the genuine concern expressed by civil society for the privacy of children. In some instances, advanced technologies, including big data analytical techniques, had been deployed and/or contemplated. The Special Rapporteur therefore respectfully draws the attention of the Government of France to the findings and recommendations contained in his reports on big data and open data[22] on gender and privacy,[23] as well as the findings and recommendations contained in his report on privacy and children to be submitted to the Human Rights Council at its forty-sixth session, in March 2021.**

F. Harmonizing federal and state legislation, policy and practice

88. **As France is not a federal State, there do not exist the same concerns that the Special Rapporteur has expressed separately in the respect of federal States like Argentina, Germany and the United States.**

G. Role of France on the international stage

89. **The Special Rapporteur notes that France has signed the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, thereby signalling its intention to adhere to that Convention as amended, but notes also that it has not yet ratified the Protocol. The Special Rapporteur, mindful**

[18] Error !Hyperlink reference not valid.A/74/277, annex.

[19] See www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/MediTASFINALExplanatory Memoradum1.pdf.

[20] A/74/277.

[21] A/HRC/43/52.

[22] A/72/540 and A/73/438.

[23] A/HRC/43/52.

also of the disruption caused by the COVID-19 pandemic, strongly recommends that the Government of France follow up on its intent and ratify the Protocol without further delay.

90. **The Special Rapporteur strongly encourages the Government of France to take a leading role in seeking the widest possible international consensus on matters regarding privacy and, especially, the safeguards and remedies that should be applicable in cases of government-led surveillance. Since January 2020, France is now the only State to be both a permanent member of the Security Council and a member of the European Union. This is a position of grave responsibility, especially when faced with two separate initiatives before the General Assembly dealing with matters relevant to State behaviour in cyberspace. The Special Rapporteur notes with satisfaction the participation by the Ambassador for Digital Affairs of France in the work of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. Together with the United Kingdom, France is also the only other member of the Security Council attempting to adhere to the standards of protection of privacy in matters of national security set out in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as amended. The Special Rapporteur sees France as being especially well-positioned to take a leadership role in building bridges between Europe and the United States, as well as between Europe and the rest of the world, in matters concerning privacy and surveillance.**