Bulgarian Public Authorities Do Not Respect Privacy When Using Secret Surveillance System: The Strasbourg Court Condemns Sofia (For the Second Time) For Violation of Article 8 of the European Convention on Human Rights

Author Details:
Marco BUCCARELLA
University of Foggia – Department of Law, Foggia, Italy
E-mail: marco.buccarella@unifg.it

Abstract
In the last few years, the European Court of Human Rights (ECtHR) has been asked many times to examine different aspects of the Council of Europe’s (COE) Member States’ (secret) surveillance legislation, especially with reference to the use of mass secret surveillance system against their own residents and to the bulk surveillance system or interception of electronic communications coming from abroad. On 11 January 2022, in Ekimdzhieva and Others v. Bulgaria (no. 70078/12), the ECtHR ruled that Bulgarian law is incompatible with the right to private life as anchored in Article 8 of the European Convention on Human Rights (ECHR), due Bulgaria appeared unable to provide effective guarantees that its citizens would not be subjected to “abusive” surveillance by the public authorities. The aim of this paper is to investigate the reasons of that judgment, in order to understand the impact of ECtHR ruling on international legal framework. The first part of the paper analyses the right to privacy in the international legal framework. The second part of the paper investigates the factual and legal background of Ekimdzhieva and Others v. Bulgaria dispute and the reasons expressed in the judgment published on 11 January 2022 by the Strasbourg Court. Moreover, it presents some critical reflections on the relevance of European Union’s personal data legislation and on compatibility of bulk surveillance systems with international legal framework.

Keywords: secret surveillance system; privacy; bulk surveillance system; European Court of Human Rights; Bulgarian legislation.

Introduction
By a judgment of more than one hundred pages, published on 11 January 2022 and finalized on 11 April 2022, the Fourth Chamber of the European Court of Human Rights (the “EctHR” or “Strasbourg Court”) ruled unanimously on the illegality of the legislation in force in Bulgaria on secret surveillance, for violation of Article 8 of the European Convention on Human Rights (ECHR), regulating “the right to respect for private and family life”. The expression “secret surveillance” refers generically to the possibility, for the State, to use tools to exercise a secret control activity on the individual (through different surveillance tools), with a consequent almost total intrusion into the private life of the same. Obviously it is an activity proper to the police state and therefore substantially admitted, in the rule of law, only where strictly necessary, subject to the existence of appropriate guarantees to protect the interested parties. The finding of incompatibility of the Bulgarian legislation with the ECHR, as found by the Court in “Ekimdzhieva and Others v. Bulgaria” (Application no. 70078/12).
This is the second sentence of the Strasbourg Court against the Bulgarian secret surveillance, following that handed down by the Fifth Chamber on 28 June 2007, regarding the dispute “Association for European Integration and Human Rights and Ekimdzhieva v. Bulgaria” (Application no. 62540/00). The judgment in question, therefore, is part of the case-law concerning the use of secret surveillance systems by a State against citizens, whose legitimacy, in the abstract, was first recognized on 6 September 1978, by the judgment defining the judgment “Klass and Others v. Germany” (Application no. 5029/71). The problem of the balance between rights (security and privacy) is of great importance today, given the increasing use by national authorities of increasingly intrusive technological tools.
Before analyzing the events at the origin of judgment 70078/12 and therefore the salient points of the verdict of 11 January 2022, it is necessary to dwell briefly on the legal instruments that, in the international context,
are important with respect to the use of secret surveillance systems by public authorities\(^1\). It should be specified that is not possible to deal here the different problem of the use of surveillance by private subjects (completely unrelated to state surveillance systems) and parastatal subjects (partially unrelated to public power). The question of the protection of fundamental rights in the exercise of private (and not only public) power was also addressed by the ECtHR in the dispute “Vukota-Bojc in Switzerland”, Application no. 61838/10, judgment of 18 October 2016.

**Right to privacy in the international legal framework**

Historically, the protection of the rights of the *civis* has always represented a limit to the exercise of public power. On the other hand, the exercise of this power for *security* reasons has raised increasingly frequent questions over the years in terms of balancing fundamental rights. As far as this is relevant to the ruling in comment, the carrying out of interception and surveillance activities by state authorities, for security reasons, meets an important limit in the protection of the privacy of individuals. In this perspective, with respect to the application of surveillance measures against natural and legal persons, the international legal instruments which recognize the right to privacy and its corollary (the right to the protection of personal data) are really important.

In the international legal framework, the right to “respect for private life” is recognized by Article 12 of the Universal Declaration of Human Rights and Article 17 of the Covenant on Civil and Political Rights (the first binding provision adopted by the United Nations). As a general rule, this is a right which may be restricted for reasons relating to the protection of national security. In particular, since Article 17 of the Covenant on Civil and Political Rights does not provide for an express derogation clause for the freedom in question, the possibility of limiting privacy in exceptional cases is evident from Article 4 (2) which does not include this right among those absolutely mandatory. On the other hand, the practice of the UN Human Rights Committee shows that privacy can be limited not only in the event of danger or exceptional emergency, but also to protect the “interests of society”, which include economic, social and cultural reasons. However, it should be noted that, in order for any restrictions on privacy to be considered compliant with the Pact, it is always necessary to respect the criteria of legitimacy and non-arbitrariness: security measures must be based on clear legal provisions and prove necessary and proportionate in order to be pursued.

Continuing the analysis of the international legal framework, it is then necessary to dwell on the ECHR and on the aforementioned Article 8, essentially aimed at protecting against arbitrary interference in private and family life, in the home and in correspondence by a public authority. This provision recognizes the right to respect for private life and to the protection of personal data, regulating the conditions under which any interference can be considered legitimate. A milestone for understanding the scope of Article 8 ECHR is the aforementioned judgment in “Klass and Others v. Germany”, where the Court, in par. 48, acknowledged that «Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime».

The admissibility, in the abstract, of surveillance systems by the State must, however, be correctly “interpreted” in the light of the technological developments that have affected intrusive tools, as also underlined by the Strasbourg Court in the most recent judgment in “Szabó and Vissy v. Hungary”. In this sense, the technological advances that have followed one another over the years since the Klass judgment require much stricter attention and control on respect for the rights guaranteed by the ECHR. In demanding first of all that there be a legislative basis legitimizing the use of secret surveillance measures and therefore a “contraction” of privacy, the Court, over the years, has then specified that this legislation must be clear and detailed, too offering minimum safeguards avoid abuses of power. This implies, from the point of view of the use of technological tools, that the legislature must clearly and specifically define the technology
permitted and the methods of its use, as well as the legitimate objectives pursued in accordance with Article 8(2) of the ECHR. For example, in the case of interceptions, the regulations must provide for the following minimum guarantees against abuses of power: the definition of the nature of the crimes that can give rise to an interception decree; the specification of the categories of persons whose telephone users may be intercepted; an express duration limit for the application of the measure; the procedure to be followed for the examination, use, and storage of the collected data; the precautions to be taken when communicating data to other parties; the circumstances in which records may or must be deleted or destroyed (see: ECtHR, Roman Zakharov v. Russia, Application no. 47143/06, judgment of 4 December 2015, §231).

In short, although there is a certain margin of appreciation for the national legislature with regard to the choice to provide for a surveillance system, the public authorities do not enjoy unlimited discretion, since they cannot, for example, adopt measures presumably considered appropriate on the basis of generic purposes of combating espionage and terrorism. Surveillance is in fact the exception to the protection of a human right as well an interference in the private life of citizens. So, any derogation from this right requires States first of all to provide guarantees against possible abuses and, secondly, to limit the use of intrusive measures only to cases where it is strictly necessary, for the protection of democratic institutions. Article 8 ECHR has therefore been used by the Court over the years as a benchmark for assessing the legality of the control systems used by the States, mostly concerning strategic surveillance tools via GPS and telephone or e-mail interception. In this sense, for example, the Court has invalidated by contrast with art. 8 ECHR the Hungarian anti-terrorism legislation of 2011, by which a secret surveillance system was introduced without providing adequate safeguards to protect the persons concerned.

To conclude the brief examination of the legal context of reference, it is useful to recall Articles 7, 8 and 52 of the Charter of Fundamental Rights of the European Union, which protect – like Article 8 of the ECHR – the right to respect for privacy and the protection of personal data within the EU.

**The processing of personal data collected through secret surveillance tools**

Another issue, linked to the use of secret surveillance tools, concerns the processing of data collected through those control systems.

In this regard, reference should first be made to Council of Europe Convention No 108, the first legally binding international instrument on the processing of personal data, even applicable in the case of processing carried out by the authorities for the prevention, detection and repression of crimes. Public legislation on secret surveillance must also expressly regulate the procedures to be followed for the storage, access, examination, use, possible disclosure to third parties and destruction of the data collected.

With regard to the processing of personal data law in the legal framework of the European Union (EU), it should be noted that the personal data processing carried out for needs related to the protection of public order and security (as in the case of the use of secret surveillance systems) have been removed from the discipline of the General Data Protection Regulation 2016/679 (General Data Protection Regulation or GDPR). The GDPR, by its express provision, is not applicable to the processing of personal data «by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security» (art. 2(2)d) and «to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security» (recital 16). It is not possible to deal here the discussed issue of the issues in practice related to the concept of “national security”, so we will limit ourselves to specifying that, in relation to the aforementioned activities, the EC Directive 2002/58 is applied – for the conservation of the data collected – and, with more general scope, the EU Directive 2016/680, as a legal instrument specifically identified by Recital 19 of the GDPR. This directive is part of the so-called data protection package presented by the European Commission in 2012 and regulates, specifically, the processing carried out by the competent authorities for law enforcement and crime prevention purposes. However, it should be noted that in the discipline of the GDPR will apply, the event that these authorities process personal data for different purposes, incompatible and additional to those indicated above, or if unauthorized persons process data for the purposes of preventing and combating crime.

http://www.ijmsbr.com/
In the light of the synthetic analysis carried out so far with reference to the international legal framework, it is possible to observe how the EU member states, in principle, can provide, through their own regulations, for the use of secret surveillance systems; moreover, the protection of security and the protection of public order are fields of competence in which, traditionally, the national authorities enjoy a particular margin of discretion. However, States, with a view to preventing abuse, have the burden of providing citizens with adequate information about the conditions and circumstances that legitimize the choice to use secret surveillance measures and, therefore, process the data collected accordingly.

**Factual and legal background of the recent judgment in the ECtHR ruling no. 70078/12**

The ECtHR dispute no. 70078/12 stems from the appeal brought by two Bulgarian citizens, lawyers Mihail Tiholov Ekimdzhiev and Aleksandar Emilov Kashamov, and by two non-governmental organizations (NGOs) committed to the protection of human rights, namely “Association for European Integration and Human Rights” and “Access to Information Foundation”. The applicants complained that they could be subject to the unlawful secret surveillance measures provided for by the Bulgarian legislation, by reason of the nature of their activities. As the Court pointed out in its judgment of 11 January 2022, however, none of the four applicants has ever claimed, let alone demonstrated, that they have actually been monitored or that they have actually found that they have had undue access to their electronic communications by law enforcement authorities. The two Bulgarian lawyers and the two ONHs merely argued that their electronic communications could have been the subject of abusive access by the police, in application of national legislation which, in the abstract, violates the “right to respect for private life” (Art. 8 ECHR) and does not provide for effective remedies against the use of unlawful surveillance measures (Art. 13 ECHR).

In Bulgaria, the relevant rules are laid down in the provisions of the Special Surveillance Means Act 1997, Articles 172-177 of the Code of Criminal Procedure, sections 304-310 of the Electronic Communications Act 2007 and the internal rules of operation of the National Bureau for Control of Special Means of Surveillance (that is a State Administration in charge of monitor on the use of surveillance tools, together with a Parliamentary Committee ad hoc and the judge who issued the warrant). In essence, these laws regulate, among others, the use of visual surveillance and environmental surveillance systems and telephone and electronic communications. The use of such intrusive tools is permitted, on behalf of the court, exclusively for reasons of national security or where this is necessary in order to prevent or ascertain “serious intentional offences” pursuant to Article 93(7) of the Bulgarian Criminal Code, i.e. offences for which a sentence of more than five years imprisonment is foreseen. A list of such crimes is contained in section 3(1) of the Special Surveillance Means Act 1997 and in section 172(2) of the Bulgarian Code of Criminal Procedure, which expressly refers to the offences of terrorism, murder, embezzlement, racketeering, desertion in time of war and illegal trafficking in drugs or nuclear materials. Regarding data retention by providers providing communication services, Bulgarian legislation (section 251b et seq. of the Electronic Communications Act 2007 and Art. 159a of the Code of Criminal Procedure) requires the retention of such kind of personal data (collected through intrusive tools) for a period of six months. Law enforcement agencies, upon a mandate issued by a district court or by judges delegated for this purpose, are authorized to access all data collected by subjects operating in the field of communication services. Supervisory powers in this area are entrusted to a parliamentary committee and, in some respects, also to the national authority for the protection of personal data.

As regards the recognition of the status of victims to the four applicants under Article 34 ECHR and therefore the admissibility of the proceeding before the ECtHR, the Strasbourg Court has applied its settled case-law, according to which the lodging of actions is also allowed by the so-called victims, potential, i.e. those who can reasonably be considered to be affected by a measure and are unable to prove it. This is a “substantialist” approach that the Court has developed over the years with a view to ensuring effective protection of the rights recognized by the ECHR, that is, to prevent conventional freedoms from being placed on a merely abstract or hypothetical level. In the dispute in question, the Court found that the mere existence of the legislation in force in Bulgaria on secret surveillance – as referred to above – interferes with the private life of the applicants. Indeed, there are provisions which may lead to potential abuse by the police and other public authorities, without providing adequate means of judicial protection for legal persons.
The illegality of the current Bulgarian legislation on secret surveillance

In the face of an action expressly alleging violation of two provisions of the ECHR, the Strasbourg Court assessed the lawfulness of the Bulgarian legislation only in the light of Article 8 ECHR, also holding that it was not necessary for the purposes of the proceedings to also rule on possible violations of Article 13 ECHR. As already said in the Introduction paragraph, the Court has taken care to verify both the lawfulness of the secret surveillance systems themselves and the lawfulness of the methods of accessing and storing data processed by communication service providers and transmitted to law enforcement agencies. Both evaluations were conducted through the same “test”, aimed at verifying the existence of sufficient guarantees (suitable to prevent abuse) also with respect to the concrete functioning of the intrusive tools that can be used. This test consists in the evaluation of the regulations in the same way as the following seven elements, as enucleated by the case-law of the Court: a) knowledge and accessibility of the legislation by citizens; (b) legal bases on which the use of secret surveillance tools and access by law enforcement agencies to data processed by communication service providers are based; c) the temporal duration of the surveillance measures and methods of processing the data consequently collected by the police; (d) the procedure to be followed in order to obtain authorization for the application of those measures; (e) arrangements for implementing the secret surveillance mechanisms; (f) the procedure for notifying the persons concerned; (g) remedies which may be remedied by the persons concerned.

As regards the first assessment parameter (a), the Strasbourg Court welcomed the clarity and accessibility of the general rules, but found that the rules on the storage and destruction of data obtained through secret surveillance systems had not been published. With regard to the legality of the legal basis (b), the Court has focused on the vagueness of section 12 of the Special Surveillance Means Act 1997, in which it provides that individuals or objects related to national security may be subject to secret surveillance measures. The generality of the term “objects” lends itself to an interpretation which may justify the application of surveillance measures against any object, such as, for example, the entire database of police forces. With regard to the duration of the applicable measures and the processing of the data collected accordingly (c), the Court pointed out that surveillance tools may be authorized for a period of up to twenty-four months, for reasons of “national security”; however, this concept is not duly specified in law. With regard to the processing of the collected data, the Bulgarian legislation has been defined as lacking in relation to the discipline on the destruction of data, also due to the absence of protections for client-lawyer communication, as a rule subject to total confidentiality. The Court, then, in analyzing the procedural procedure governed by the legislation (d), highlighted several fundamental critical issues, as demonstrated by the “blanked and generalized reasons used in Bulgaria over the last decade, as the basis for the use of surveillance tools. The general nature of the reasons translates, from a practical point of view, into the possibility of adopting unjustified and therefore illegitimate surveillance measures; this occurred, for example, when the Bulgarian judicial authority issued surveillance warrants with reference to citizens participating in the 2020 anti-government protests. In relation to the implementation aspects (e), the ECtHR, in addition to having found the lack of legal competence among the officials of the aforementioned National Bureau for Control of Special Means of Surveillance, censured the absence of *ex post* controls by the judicial authority, to which the law allows to adopt corrective measures exclusively in the context of the related criminal proceedings. Although the main parameter of judgment was art. 8 ECHR, it should be noted that the Court also focused on the application of EU Directive 2016/680. With regard to this legal instrument, the judgment in the epigraph established the omitted involvement of the Commission for Personal Data Protection (CPDP) and the Supreme Judicial Council, which should instead be responsible for supervising the processing of data collected through surveillance systems. As regards the procedure for notifying persons under surveillance (f), the Court, in reiterating that it is necessary to inform the persons concerned whenever this does not prejudice the investigation, pointed out that the Sofia legislation is deficient in several respects. In particular, Bulgarian law requires notification only where surveillance has been declared unlawful and exclusively in respect of natural persons, without therefore providing for anything for legal persons. In addition, the main rules on notification are not coordinated with EU Directive 2016/680, since they lack any reference to the information burden and the rights due to the data subject, including the right of access to their data. Finally, with regard to the question of “remedies” (g), the Court found that the Bulgarian provisions on the matter,
while providing in the abstract for damages against any unlawful practices of secret surveillance, are not fully compliant with Art. 8 ECHR, as they are not applicable to legal persons and in any case not supported by a legitimate notification system (for the reasons indicated above).

The unlawfulness of the processing of data transmitted to the public authorities by communication service providers

As already mentioned, also with regard to the second profile of illegitimacy ascertained with respect to Article 8 of the ECHR (processing of data transmitted to law enforcement agencies by communication service providers), the Court used the seven elements of assessment set out in the preceding paragraph. With regard to the accessibility, clarity and legitimacy of the legal basis (a, b), the judgment validated the regulations in force in Bulgaria. With regard to the methods of processing the data collected (c), the ECtHR has, however, found that the provisions imposed by EU Directive 2016/680 had not been published, rules governing the issue of access by data subjects, also and above all to data used in criminal proceedings. With regard to the authorization procedure for access to data held by communication service providers (d) in the judgment, it was pointed out that law enforcement agencies are not required to provide a justification in support of the request for that permission and also the judicial authority is not required to justify any decision to issue a warrant to that effect. With regard to the issue of the supervision of the processing of data transmitted by communication service providers (e), the Court re-proposed the critical issues already summarized before with respect to the bodies only “formally” in charge of carrying out a verification, inspection and possibly corrective activity. Finally, also with regard to the procedure for notifying the persons concerned (f) and any remedies envisaged (g), the Strasbourg courts found different problems, such as to confirm the non-compliance of the legislation with Article 8 ECHR.

On the basis of all the critical issues briefly summarized here, the ECtHR has therefore found the illegality of the Bulgarian regulations, which, although theoretically governing a «targeted» and not «mass» surveillance system, do not fully meet the “quality of law” requirement and are incapable of keeping the “interference” entailed by the system of retention and accessing of communications data in Bulgaria to what is necessary in a democratic society.

That declaration of illegality was held by the Strasbourg courts to be sufficient just satisfaction for any non-pecuniary damage suffered by the applicants as a result of the two breaches of Article 8 of the Convention, within the meaning of and for the purposes of Article 41 ECHR.

For the rest, Bulgaria was ordered to pay a total of € 3,290.69 and, of course, to adapt its legislation on secret surveillance to the requirements of the Court, in accordance with Article 46 ECHR. It should be noted that the expected new “corrective” measures – which Sofia will have to adopt in execution of the recent judgment – will be added to those approved at the outcome of the aforementioned controversy Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria.

Conclusions

The judgment of 11 January 2022 essentially offers two points for reflection of general application, to be developed in the light of the international legal framework.

The first consideration concerns the recognition, also in the field of privacy and data protection, of the correlation between EU legislation and the legal instruments of the Council of Europe. As noted in the previous paragraphs, the ECtHR also referred in its decision to an EU legal instrument, namely Directive 2016/680. Although the “formal” parameter of legality was, for obvious reasons, Article 8 ECHR, the reference to the abovementioned Euro-Union source is relevant for two interrelated reasons. First of all, the importance of the ruling is explained by the fact that Directive 2016/680 has rarely been the subject of judgments of the Court of Justice of the EU. Secondly, from a more general point of view, it should be noted that the reference to a legal instrument not adopted within the Council of Europe constitutes a “recognition” of the importance of EU legislation on data protection, also with regard to the detection of possible violations of Article 8 ECHR. In practice, this recognition can provide the EU institutions with guidance on the future implementation of existing legal instruments, insofar as the Court has expressed its views on important issues, for examples ignoring the formal content of the Sofia legislation and choosing rather to
assess (negatively) also its “practical” dimension that is to say concrete implementation in the context of the use of secret surveillance tools.

The second reflection concerns the “presupposition” of the analysis carried out by the ECtHR in the judgment in question. The Strasbourg judges found the unlawfulness of Bulgarian legislation on the assumption that it should have constituted – mostly in theory – a discipline for “targeted” and not mass surveillance, consequently finding, in this specific perspective, a lack of guarantees to protect citizens. However, the Court did not directly address the issue of the admissibility of bulk surveillance systems, which leaves unanswered a fundamental question: whether and under what conditions mass secret surveillance systems are compatible with the essence of democratic societies. Should legislation be considered unlawful, for violation of the ECHR, because it provides for a mass surveillance system in itself or only to the extent that it does not include sufficient guarantees to protect privacy? Also in other more recent judgments, including the ruling on the mass espionage of communications data carried out by the British Government Communications Headquarters (ECtHR, Big Brother watch and others v. the United Kingdom, Application no. 58170/13, 62322/14 e 24960/15, judgment of 25 May 2021), the Strasbourg judges focused on verifying the guarantees that may be provided for by the legislation under complaint, without however expressly clarifying whether the binomial “mass surveillance-respect for privacy” can abstractly be considered compatible with international legal framework and therefore legitimate. This is a question that – regardless of the positions of merit – is destined to take on increasing importance, given the incessant development of technology and the potential use of artificial intelligence algorithms to implement mass surveillance systems, including by private individuals and legal entity.

References

CCPR, General Comment No. 16: Article 17 (Right to Privacy) – The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation, 8 April 1988.
Crosston M., Cyber Colonization: The Dangerous Fusion of Artificial Intelligence and Authoritarian Regimes, in Cyber, Intelligence and Security, 1/2022, 149-171.
Dimitrova D., Ekimdzhiev and Others v. Bulgaria: secret surveillance and electronic communications surveillance only with adequate safeguards, or nothing new under the sun, in StrasbourgObservers.com, 2 March 2022.
European Data Protection Supervisor (EDPS), Executive summary EDPS Opinion on the data protection reform package, 7 March 2012.
Ruotolo M., La sicurezza nel gioco del bilanciamento, in Astrid Rassegna, 2009, 1-49.
Seminara L., Sorveglianza segreta e nuove tecnologie nel diritto europeo dei diritti umani., in Medialaws, 2/2018, 132-145.