First published 2017
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
711 Third Avenue, New York, NY 10017

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
Names: Friedewald, Michael, 1965– editor.
Title: Surveillance, privacy and security : citizens' perspectives / edited by Michael Friedewald, J. Peter Burgess, Johann Cas, Rocco Bellanova and Walter Peissl.
Description: Abingdon, Oxon ; New York, NY : Routlede, 2017. |
Series: PRIO new security studies | Includes bibliographical references and index.
Identifiers: LCCN 2016043185| ISBN 978-1-138-64924-8 (hardback) | ISBN 978-1-315-61930-9 (ebook)
Subjects: LCSH: Electronic surveillance—Social aspects. | Electronic surveillance—Government policy. | Privacy, Right of—Social aspects. | National security—Social aspects.
Classification: LCC HM846 .S884 2017 | DDC 323.44/82—dc23
LC record available at https://lccn.loc.gov/2016043185

ISBN: 978-1-138-64924-8 (hbk)
ISBN: 978-1-315-61930-9 (ebk)

Typeset in Bembo
by FiSH Books Ltd, Enfield

6 The deployment of drone technology in border surveillance

Between techno-securitization and challenges to privacy and data protection[1]

Luisa Marin

Introduction: the EU and the techno-securitization of borders

It is commonly acknowledged by scholars that the Europeanization of national migration policy is caused by national failures in the domain, and that European migration policy can be explained through the theory of securitization. According to the latter, migration and migrants are framed, in political discourses (Weaver, 1995), by security actors (Bigo, 2000) and through practices (Balzacq, 2008), as security threats. This conceptual framing of migrants as security threats has led Member States and the EU to react to defend internal security from those alleged external threats. Globalization has turned the world into a 'global village', where goods, capitals and information circulate across the globe. However, this has not helped to decrease persistent inequalities between regions of the world. Western states, or the states of the Global North, have consolidated their interest in regulating the human dimension of globalization, i.e., human mobility. At EU level, the governance of human mobility aims at controlling the overall phenomenon of human migrations essentially by increasingly limiting legal migration and consequently fighting against irregular migration. This has attracted a number of criticisms, captured by the label 'Fortress Europe' and depicting Europe as an inaccessible fortress.

Within this process, border surveillance has gained relevance too. The EU and Member States are investing in technological applications, ranging from biometrics to databases, to drones and satellites. The aim is to deploy the most effective technological means in the attempt to face the security threats allegedly coming from outside and to make such controls more efficient. In the past few years, we have witnessed a consolidation of securitization discourses and practices, namely with a stabilization of the trend of deployment of all the available technological tools in border surveillance, which is here framed as techno-securitization (Marin, 2011; Marin 2016a). Just to mention some of the latest developments, the legislative package on Smart Borders, consisting of an Entry-Exit System (E-ES) and of a Registered Travellers Programme (RTP) has been presented (European

Commission, 2013a and European Commission, 2013b). It is currently being discussed in the legislative process. The Smart Borders package is meant to facilitate movement for selected categories of (low risk) travellers and to store biometric data of third-country nationals on entry and exit from the EU, in order to map the 'overstayers'. Alongside this, the European Border Surveillance System (EUROSUR) has been created. As suggested by some scholars, the EU and Member States are consolidating (or transforming) the 'high-tech fortress' (Marin, 2011) or 'cyber-fortress' (Guild *et al.*, 2008) around Europe.

UAVs (Unmanned Aerial Vehicles) or RPAS (Remotely Piloted Aircraft Systems), simply known as drones, are part of this process. In the context of border surveillance, this techno-securitization takes shape in a militarization of border surveillance through the deployment of warfare assets and technologies for civilian purposes. It is functional to the extra-territorialization of border controls, in a never-ending attempt to move (the controls on) the borders outwards and, ultimately, to prevent undesired migrants from reaching Europe (Marin, 2016a). In this perspective, and thanks to the surveillance technologies they can carry, drones can contribute to the attainment of the objectives of EU border controls, i.e., to reducing the number of migrants illegally entering the EU, by preventing undocumented and undesired migration and, of course, also contributing to the fight against cross-border crime. Drones can provide information to border guards present on the ground, be it by sea or by land, and therefore help to make border surveillance a proactive policy, rather than a reactive one. These ground patrols, thanks to the information acquired by drones, could then take control of migrants. In the case of migration by sea, they could support them in case of distress, taking them to the nearest port, but also re-direct them to international seas or to the authorities of cooperating third countries, if bilateral agreements so provide.

This chapter will focus on the deployment of drone technology (DT) in border surveillance. The aim is to explore how it affects the relation between security on the one side, and privacy and data protection on the other side. Having introduced the theory of techno-securitization, the chapter then presents and analyses the impact of drone technology on the techno-securitization of borders. It starts by examining how the metamorphosis of the drone from a battlefield tool to a civilian asset is taking place, and then it focuses on the EUROSUR border surveillance network and on actual cases of deployment of drones in border surveillance operations. The analysis of the current practices aims to provide information on the deployment of drones and, second, to elaborate on the impact of DT on privacy and data protection obligations. What challenges for privacy arise from the current regulation on surveillance at the borders? Is the legal framework equipped for those challenges? The chapter concludes by recalling the challenges posed by the techno-securitization of its borders for privacy and data protection.

The deployment of drones in border surveillance and their contribution to pre-emptive techno-securitization

The metamorphosis of the drone: from warfare drone to a border defence drone

If the literature so far has been focusing on the deployment of drone technology in warfare, the 'metamorphosis' of war drones into a civilian 'tool' is more recent and still ongoing: therefore, it is only starting to receive the attention it deserves in the scholarly debate (Custers, 2016; Završnik, 2016). The current work aims at filling this gap in the literature, namely elaborating on the deployment of drones in border surveillance and their impact on the function of border surveillance, in the perspective of the relation between security on the one side and privacy and data protection on the other.

How did we get to the transfer of drone technology to the civil domain? Drones are best known for the targeted killing programmes carried out by Israel and the US in Middle East theatres of war, with CIA's famous 'personality strike' and 'signature strike' programmes. These triggered reactions within the international community for their dubious compatibility with the principles of proportionality, precaution and necessity in relation to civilian casualties (Alston, 2010; Rosén, 2013). Alongside this, targeted killings with drones have been accused of changing warfare, by lowering he threshold to engage with it (Alston, 2010; Human Rights Watch, 2012). However, drones were first developed as surveillance instruments and have been used for intelligence and reconnaissance since the Vietnam war; attack drones being the armed variant of drones, UAVs are, first of all, intelligence, surveillance, target acquisition and reconnaissance (ISTAR) devices/tools.

So, what is the peculiarity of drones and what makes them attractive for civilian and commercial uses? If the topic of the commercial exploitations of drones will remain out of the scope of this research, this section will focus mainly on border surveillance, as one of the main governmental exploitation of drones.

One of the main assets of drones – in addition to their being unmanned or remotely piloted aircrafts – is that they perform tasks usually characterized as the '3 Ds': dull, dirty and dangerous. From the technical viewpoint, they are surveillance tools and they enable the coverage of vast and remote areas that would be more difficult to reach with traditionally piloted aircrafts. For example, a Predator can fly for up to 20 hours. Drones can be equipped with cameras and thermal detection sensors. These can find small objects at a distance of 60,000 feet and detect humans moving across woods, also under foliage (Haddal and Gertler, 2010). Therefore, the attractiveness of drones is that they enable enhanced surveillance, compared to manned aircraft. Their value also lies in the amount of information and data that they can be allowed to collect, and in the use of those data from the deploying or, more correctly, the benefiting agency.[2]

Second, piloting at a distance makes it possible to keep pilots' lives safe, away from risks related to weather and other natural hazards. Another advantage of the unmanned drone is that the aircraft can stay airborne according to logic and necessity totally independent from human fatigue and pilots' shifts. This remoteness is

often seen as a benefit for the agency deploying the drones. However, it does not consider that other lives might be exposed to risks deriving from the operation of an aircraft instead of the deployment of a manned guard, for example (Gertler, 2012). One risk is the dehumanization of the surveilled (Marin, 2016b; Finn *et al.*, 2014).

Other reasons put forward to defend the deployment of drones in border surveillance concern economic arguments. Proponents of drone technology in border surveillance (in Europe: industry stakeholders, national administrations, Frontex, European Defence Agency and European Commission) argue that this technology is potentially cheaper than surveillance carried out with traditional manned aircraft.[3] Second, once developed and implemented, drones would make border surveillance operations less expensive, both in terms of human resources and material assets deployed, allowing for a rationalization of the resources employed (Gertler, 2012). In times where public agencies face financial restrictions, this economic argument is always attractive. Its actual validity is however strongly challenged by the American experience, where drones acquisition programmes have been suspended for financial reasons caused by inaccurate forecasts on the overall maintenance expenditures for drones.[4]

Surveillance networks in border surveillance: EUROSUR

The actual deployment of drone technology in border surveillance by EU Member States started late in comparison with the US, which have been using drones in border surveillance since 2004 (Marin, 2016b). However, it is rapidly increasing (Hayes *et al.*, 2014). The next section will first present the legal framework enabling the deployment of drones in border surveillance, and the ensuing sub-section will present practices and examples of the same. Here drones are considered a crucial technology, alongside others, in order to reshape surveillance of the maritime environment.

EUROSUR is a surveillance system whose aim is to sustain better border management of the EU's external borders. Surveillance is carried out by Frontex with the Member States' border authorities (European Commission, 2011; European Commission, 2013c). In a broader perspective, EUROSUR is part of the creation of a Common Information Sharing Environment (CISE) for the enhancement of maritime security. Drone deployment in border surveillance at EU level is part of a policy that aims at strengthening the surveillance of external EU borders – first, as a tool to control irregular migration, and second, within the context of EU's integrated maritime policy, which is setting up a Common Information Sharing Environment (CISE) since 2009. For this reason, shortly after the creation of Frontex, the Member States, the Council and the European Commission examined the feasibility of EUROSUR as 'a common technical framework to support Member States' authorities to act efficiently at national level, command at national level, coordinate at European level and cooperate with third countries in order to detect, identify, track and intercept persons, attempting to enter the EU illegally outside border crossing points' (European Commission, 2008: 1). In December

2013, less than 2 months after the Regulation was passed, EUROSUR was already operational for 18 EU member states at the southern and eastern external borders and Norway.

EUROSUR is composed of the National Situational Pictures, of the European Situational Picture and of the Common Pre-Frontier Intelligence Picture (CPIP). These give an overview or representation of the situation at and outside the EU borders, including information on prevention of unauthorized migration and cross-border crime. In particular, the CPIP (Art. 11, EUROSUR Regulation) aims at providing the national coordination centres (NCC) with 'effective, accurate and timely information and analysis on the pre-frontier area.' Among others sources, the CPIP is composed of information collected by Frontex, including information and reports provided by its liaison offices; information collected via third parties; and information collected from authorities of third countries, on the basis of bilateral or multilateral agreements and regional networks via the NCC. This indicates that EUROSUR is to be used as a platform to share information and to develop the intelligence dimension of border surveillance. Here drones, among other technologies such as satellites and ship monitoring systems, would play a central role in acquiring information on what happens at and outside the borders. Increased information will lead to so-called 24/7 blue/green situational awareness and implies the technical capacity of having full information on what happens at the borders (Marin, 2016a). Drones are of vital importance for EUROSUR since they will enable acquisition of crucial information, thanks to infra-red cameras, mobile phone jammers, thermal imagining devices and video cameras (Nolin, 2012).

EUROSUR strengthens Frontex's role as 'the' intelligence hub for border surveillance. In particular, article 12 of the EUROSUR Regulation mandates Frontex to 'coordinate the common application of surveillance tools in order to supply the national coordination centres and itself with surveillance information on the external borders and on the pre-frontier era on a regular, reliable and cost-efficient basis' (Art. 12 EUROSUR Regulation). Frontex provides the national coordination centres, at their request, with information on the external borders of the requesting state and on the pre-frontier area. Frontex can elaborate this information by analysing data collected from ship reporting systems, satellite imagery and sensors mounted on any vehicle, vessel or craft. This legal basis enables Frontex to combine and analyse the data collected from ISR drone operations.

The main purpose of EUROSUR is to share information and therefore to develop and strengthen intelligence and risk management at the external borders and in the pre-frontier area with a focus on prevention. Drones are therefore an important technology enabling a shift toward risk-oriented and preventive border surveillance, as an epiphany of the techno-securitization process of borders.

Drone deployment in border surveillance in Europe: some examples

Let us now turn to some examples and practices of drone deployment in border surveillance. In this context, the information is scarce and research in this domain can only attempt to sketch some insights.

Italy, for example, is a country that deploys drones for border surveillance and security purposes. Considering that one of the layers of EUROSUR is given by the (many) National Situational Picture(s), we can think that information acquired by one country (e.g., Italy) with the deployment of drones can be used to feed the EUROSUR system. Italy owns 12 UAVs, 6 MQ-1 Predators and 6 MQ-9 Reapers or Predator B; these MALE (medium altitude long endurance) drones can stay airborne for about 20 hours. Since October 2013, drones have been part of the technical equipment of the *Mare Nostrum* operation.[5] According to the information available, drones have been deployed in the area of Lampedusa, north of the Libyan shores and also at the Southern Libyan border (with Niger, Chad and Sudan). Patrolling the sea close to Libyan borders took place within the context of the EUBAM mission, terminated in 2014 due to the war in Libya. EUBAM was a civilian mission under the Common Security and Defence Policy, aimed at supporting the Libyan authorities in improving and developing the security of the country's borders. The mission supported Libya in developing border management and security through transfer of know-how and capacity building at the operational and strategic levels (advising, training, mentoring). Patrolling the Southern Libyan border was made possible by a bilateral (Italy-Libya) Technical Agreement (TA) of cooperation of November 2013, authorizing, among other things, border surveillance activities with drones.[6] The Predators and Reapers, launched from the Sigonella Italian and NATO Air Base, in Sicily, patrolled the Southern border, probably in order to collect information and ensure earlier detection of migrants (Amnesty International, 2014).

Another example of drone deployment is offered by the EU NAVFOR MED (later renamed SOPHIA) operation. Formally speaking this is not a border surveillance operation but a 'military crisis management operation contributing to the disruption of the business model of human smuggling and trafficking networks in the Southern Central Mediterranean (…)' (Art. 1 Council Decision of 18 May 2015 (CD CFSP 2015/778 of 18 May 2015). It is a Common Security and Defence Policy (CSDP) operation, discussed and agreed upon after the Lampedusa disaster of 18 April 2015. This was the most dramatic accident after the one of 3 October 2013, in which between 700–900 migrants lost their lives at sea. It represents a turn in border controls and in the management of irregular migration through fighting human trafficking and smuggling. The goal of the mission is to disrupt the business model of smugglers and traffickers, and possibly to prevent migrants becoming the 'objects' of criminal activities. For this purpose it makes a systematic effort to identify, capture and dispose of vessels and assets used or suspected of being used by smugglers or traffickers. This is done in accordance with applicable international law, including UNCLOS and any UN Security Council Resolution' (Article 1, CD). It operates alongside Frontex coordinated JO Triton, and it coordinates with it.[7]

It is organized in phases: phase 1 concerns surveillance and assessment of human smuggling and trafficking networks in the Southern Central Mediterranean; phase 2 entails boarding, search, seizure and diversion, on the high seas and in territorial waters, of vessels suspected of being used for human trafficking or smuggling; phase

3 entails the disposal of vessels and related assets and apprehension of traffickers and smugglers. Both the second and the third phases require a UN Security Council Resolution. The progress of the operation, which according to international law requires the consent of the coastal state, is uncertain because of the situation in Libya. At the time of writing operation SOPHIA has terminated its phase 1 and phase 2A, in international waters. Phase 2B would take place in territorial waters, for which there is a need for consent by the Libyan government. However, the situation in Libya presents/creates legal and political challenges that do not allow the operation to move forward. The EU is currently supporting the formation of a Government of National Accord in Libya which might represent a partner allowing the further progress of the operation toward phase 2B and 3 (European External Action Service, 2016).

Without dealing here with the legal issues concerning this operation, one has to stress that drones are also being used in this operation, at least both by Italy and by the UK, currently for surveillance and reconnaissance. If the operation at one point moves forward, drones – technically speaking – could also be used to destroy vessels. In this case too drones, together with other heavy defence means, are used for ISR operations and appear functional to a pre-emptive turn in border surveillance and in the management of migration. This turn requires fighting traffickers and smugglers with military technology, such as satellites, sensors and drones. EUNAVFOR MED is certainly a step in this direction. It is not formally a border surveillance operation, but it aims at transferring defence instruments, assets and technology to the borders and beyond: it is defence assets placed to defend the borders. It therefore represents a consolidation of the militarization of border surveillance and a further step in the direction of its externalization to the countries of departure, contributing to the techno-securitization of borders.

Having presented the rationales for deploying drones in border surveillance (and defence), alongside the legal framework for the surveillance of borders and some practices of it, the section concludes that by using drones, governmental agencies aim at strengthening surveillance, intelligence and coordination toward anticipatory border surveillance and prevention of migration. This section illustrates that drones are a key surveillance technology in this process; together with other technologies, such as satellites, drones are functional to a process of techno-securitization of borders.

The chapter will now focus on drones' impact on privacy and data protection issues.

Enhanced surveillance by drones and its impact on privacy and data protection rights

Drones, privacy and data protection

Starting from the consideration that borders are the legal and physical spaces where states exercise control on individuals in order to maintain their sovereignty, does the deployment of drones affect privacy and data protection? This section examines to what extent enhanced border surveillance can represent an issue, and also

to what extent the legal framework addresses the high potential of surveillance of drones. It does not aim at offering comprehensive research but rather sketches some of the issues for privacy and data protection deriving from the deployment of drones (Marin and Krajčíková, 2016; Finn *et al.*, 2014).

The deployment of drones for (border) surveillance potentially challenges the privacy and data protection rights of individuals found by the surveillance devices drones carry (high resolution optical camera, infra-red thermal camera, GPS, to name some): they should be considered as mobile CCTV. The privacy and data protection risks relate to the collection of images, sounds and geo-location concerning identified and identifiable persons (Art. 29 Working Party, 2015).[8]

Drones being a sense-and-detect technology, they can indeed collect and transmit information to the drone operator, including visual data.[9] It can be information about fishermen, tourists, migrants or more generally anyone finding himself or herself in the Mediterranean. At the same time, drones make it possible to interfere with private premises (for example, a boat sailing on the sea) due to the capacity of the technology they carry to collect data without the need for a direct line of sight. Here the challenges to privacy are multiple: first of all, drones represent a risk for the privacy of persons and for their data protection rights. Second, drones represent a risk for drone users because they have – in principle – to comply with respect for privacy and data protection obligations.

As to persons' privacy rights, drones first of all make it difficult for individuals to know that they are the subjects of surveillance: there is a lack of transparency on the types of processing because of the impossibility of seeing drones from the ground; there is a difficulty about knowing the equipment on board, and monitoring for what purposes data are collected and by whom. In short, surveillance by drones complicates the exercise and enforcement of rights as constructed by the European and national regulations (Art. 29 Working Party, 2015). Such technologies could also enable the collection of data for a long period of time and across large areas; this triggers the risk of 'bulk data gathering and possible unlawful multipurpose uses' (Art. 29 Working Party, 2015: 8). The deployment of new technologies such as drones potentially represents a major interference with privacy and brings a risk of function creep. In a regulatory perspective, it is therefore important that legislators and regulators monitor the risks and consequences of the deployment of drones for surveillance. This also applies in the case of processing personal data for law enforcement purposes. Drones, together with the surveillance technology they can carry, represent 'game changers' in the direction of an anticipatory policing (Sandvik, 2016; Milivojevic, 2016). Mass data collection is functional to new practices of policing directed toward continuous surveillance, enabling determination of targets from a review of the lives and activities of a specific population (Art. 29 Working Party, 2015). So, all the more in the case of governmental activities, drones should only be used if less intrusive instruments are not suited to the achievement of such purposes. In any case, drones should not be used to conduct indiscriminate surveillance, bulk data processing, data pooling and data profiling. The legislator should avoid drones being used for signalling targets based on data analysis.

The normative framework of privacy and data protection

Border surveillance must be placed in the broad context of law enforcement functions. It is especially sensitive because of its implications for transparency of operations, enforcement of rights and also possible cooperation with third countries. Having mapped (some of) the issues related to privacy and data protection in this domain, let us turn to the normative framework, in order to see whether the legal framework covers those issues adequately.

These questions are relevant because in the EU legal order, respect for privacy and the right to protection of personal data have fundamental rights status and are codified in Articles 7 and 8 of the Charter of Fundamental Rights (hereinafter: FR) of the EU. Alongside this, Article 16 of the TFEU enshrines EU competence on data protection. Within the legislation, the Data Protection Directive 95/46/EC (hereinafter: DPD), and the Framework Decision 2008/977/JHA (hereinafter: the DPFD) on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters are core instruments. They have inspired the constitutional guarantees of the Charter of FR. The DPD and the DPFD are now in the process of being repealed by the General Data Protection Regulation and by the Police and Criminal Data Protection Directive: at the time of writing, the 'trilogues' meetings have been concluded and an agreement on a text has been reached.

The DPD is the backbone of data protection at EU level. Its scope covers 'the processing of personal data wholly or partly by automatic means'. By contrast, it does not cover 'processing operations concerning public security, defence and state security (including the economic well-being of the state when the processing operation relates to state security matters) and the activities of the state in the areas of criminal law' (Articles 3 and 13, DPD). So, the DPD allows Member States to restrict the scope of the obligations and rights protected by the DPD, if this is necessary in order to protect, among other matters, national security, public security, and for the 'prevention, investigation, detection and prosecution of criminal offences' (Article 13, para. 1, letters a), c), d), DPD).

It is not so clear how to relate border surveillance with reference to this law enforcement exception of the DPD. It is clear that border surveillance is connected to the protection of public security, and also to the prevention, detection and prosecution of crimes connected to irregular migration, smuggling and illegal trafficking. However, we should consider that this represents an exception from the application of the DPD. Alternatively, it could be framed as a limitation of the fundamental right of data protection, and any limitation to EU fundamental rights has to respect the rule of law and the proportionality principles. Second, after the *Digital Rights Ireland* judgment,[10] it should be noted that the protection of public security might not entail a generalized surveillance and storage of data of individuals without a clear relation to investigations on crime. With the *Schrems* judgment,[11] the Safe Harbour Decision, allowing for simplified transfer of personal data between EU and US commercial companies, was annulled because of its lack of compliance with privacy and data protection obligations, in light of factual

elements that emerged after Snowden's revelations. These judgments have the important meaning of requiring that surveillance measures (namely, the data retention directive) as well as data exchange agreements are embedded into the traditional guarantees of the rule of law and respect for fundamental rights, and that the trade-off between security and privacy cannot be achieved by sacrificing guarantees of privacy and data protection (van Lieshout *et al.*, 2013). Third, even if border surveillance might fall within the scope of the law enforcement exception of the DPD, both the Frontex Regulation and the EUROSUR Regulation bear provisions aimed at anchoring the processing of personal data to the national and European frameworks on data protection. To conclude, there is a need to clarify the legal framework for border surveillance activities and, vice versa, to anchor the latter activities to a legal framework capable of protecting rights but at the same time guaranteeing adequate exercise of law enforcement powers. According to the European Convention of Human Rights and to the Charter of FR, restrictions to FR must be provided for by law and must respect the requirements of necessity, of being apt to fulfil the objectives of general interests and of proportionality. The recent militarization of border surveillance, the externalization of border controls policies to TC and the further expansion of defence functions toward border control issues represent a further threat to the embedding of these operations into a strong legal framework, and might therefore, jeopardize those rights. In the future, this domain will be covered by the new Police and Criminal Data Protection Directive and this will guarantee some uniform standards, even when Member States act in purely internal situations (Finn *et al.*, 2014).

Having sketched the general framework, the domain of border surveillance offers specific provisions on data protection. Borders are not the place to invoke 'the right to be left alone'. However, the right to data protection is nevertheless a fundamental right that is separate from the right to privacy; it regulates the relation between public authorities and individuals and limits the powers of the former to the respect of rights of the latter (González Fuster and Gutwirth, Chapter 10, this volume). To this purpose, the EUROSUR Regulation and the techno-securitization of borders, by enabling extensive surveillance, potentially limit the privacy and data protection rights of the individuals involved. In the EUROSUR system, in principle 'any exchange of personal data in the European situational picture and in the common pre-frontier intelligence picture should constitute an exception' (EUROSUR Regulation, recital 13). However, Article 13 guarantees that the processing of personal data within EUROSUR is anchored to the European and national frameworks for data protection, and carried out with respect for the principle of purpose limitation. Moreover, sensitive issues remain in the cooperation of Frontex with third-country authorities (TCA) in the framework of border surveillance. In this context too, the exchange of personal data should constitute an exception. Furthermore, 'it should be conducted on the basis of existing national and Union law and should respect their specific data protection requirements'.[12] This means that data collected for EUROSUR can be transferred to TCA. This still begs the question of the fate of those data and of the persons they refer to once in the hands of TCA. Connected to this, another important challenge to data

protection emerges from the cooperation of Member States with neighbouring TC. Member States can include information gained from cooperation with TC in the national situational picture and exchange information according to Art. 20 of the EUROSUR Regulation. Article 20 provides that exchange of personal data shall be strictly limited to what is absolutely necessary for EUROSUR. Though strictly limited, the exchange of personal data is still possible, and this triggers, again, the question of the fate of those data, once in the hands of TC institutions. How can the European institutions (Commission *in primis*) and the Member States monitor the respect of data protection provisions, after they have exchanged data, e.g., with Tunisian or Libyan authorities? The threat of function creep is here. The fact that some of these agreements are secret does not help accountability and the exercise of rights. The *Schrems* judgment is of relevance here and it recalls the strict boundaries for the transfer of personal data toward TC. Cooperation with TCA does not guarantee respect for data protection principles as implemented within the EU, and, more radically, brings more fundamental challenges on the respect of human rights of migrants (Marin and Krajčíková, 2016).

Another threat represented by the deployment of drones is the so-called chilling effect: the extended and continued surveillance of broad areas could deter migrants' vessels from using a specific route and perhaps could push them to use a more dangerous route, further endangering the lives of migrants. Drones can technically follow the routes of selected vessels, take images of what the crew is doing and prevent a cell phone from receiving a signal. To sum up, the EUROSUR Regulation embeds border surveillance into the network of national and European data protection provisions. However, it cannot be forgotten that large-scale surveillance in the Mediterranean can also cause a 'chilling effect' or self-disciplining effect or even affect society's expectations and interpretations of privacy. For this reason, it is important that public and independent authorities monitor the deployment of new technological 'eyes in the sky' and surveillance systems and their impact on privacy and data protection; on the other side, law enforcement agencies should provide information on their actions in compliance with transparency and accountability.

Conclusions

The chapter has presented one of the law enforcement domains, border surveillance, where security and privacy are in conflict. As in other justice and home affairs policies, in border surveillance too the EU and Member States are investing in technological and military applications in order to strengthen the security of the maritime environment. The aim is also to prevent irregular migration and crime.

Drones are already playing a role in this context and we should expect that this technology will be developed in the future, so that their deployment will increase. Italy deploys them already and Frontex has shown interest in them and is supporting R&D in the domain. Compared to manned aircraft, drones can stay airborne for longer times and therefore can provide more complete and accurate information on what happens at sea. The proponents of this technology suggest that there

are also economic advantages: namely drones are deemed to be cheaper compared to manned aircrafts, but it is not really straightforward to calculate these economic advantages.

Drone deployment is part of a process that is consolidating a shift in border surveillance from an emergency-driven policy to an intelligence and risk management approach of border surveillance. The creation of EUROSUR, enabling national and European agencies to share information on what happens at their borders, is to be read in this process. Drones seem to be a crucial 'game changer' in the shift from reactive border surveillance toward anticipatory border surveillance, which also seems to postulate, to some extent, the cooperation of third countries.

The chapter has shown that the deployment of drones raises several issues. Drones should be considered as mobile CCTVs and therefore their deployment should be accompanied with adequate assessment of their implications. Second, in the current legislative setting, data protection issues in this domain are subject to national legislations: the domain of law enforcement and criminal law is indeed representing a derogation to the European Data Protection Directive. Currently, there might be divergences and different rules in place at national level. In the future, the domain will be covered by the draft Police and Criminal Law Data Protection Directive and this will represent a common ground to which all national law enforcement agencies will have to adhere.

Second, in spite of the guarantees of the EUROSUR Regulation (EUROSUR's primary aim is not to collect personal data). In the Regulation there are avenues for sharing data with TCA, both for Member States but also for Frontex. Indeed, EUROSUR provides for a common pre-frontier intelligence picture to be fed with information received by TCs, which is a problematic issue, in light of the level of rule of law and protection of rights of migrants in those states. Once the data are transmitted to the third countries, there is a risk of function creep that can hardly be controlled from Europe. So, even if constrained by fundamental rights provisions on data protection, increased surveillance of borders, and the possibilities for cooperation with third-country authorities, challenge the safeguards provided by the European legislations. Third, it is important that transparency is safeguarded, as without transparency the enforcement of rights is prejudiced. The chapter therefore suggests that with the deployment of drones in border surveillance there are several instances of tensions between privacy and data protection, which are at the core of the European and national legal orders. For these reasons, it is important that the deployment of new technologies in law enforcement domains is adequately monitored in order to assess their implications.

Notes

1 The author thanks the editors for useful comments on a previous draft of the chapter. The usual disclaimer applies.

2 The deploying and benefiting agencies could be different actors. For example, a deploying agency might well be the Air Force, while the benefiting agency might be the Ministry of Interior.

3 In Gertler (2012, p. 5) one can read: 'Congress has noted that, "while the acquisition per unit cost may be relatively small, in the aggregate, the acquisition cost rivals the investment in other larger weapon systems'." Second, while a Predator vehicle costs $4.5 million, the Predator system, including four air vehicles and control equipment, costs over $20 million (Gertler, 2012).
4 Marin and Krajčíková (2016, p. 110) (quoting Sternstein, 2012), about problems experienced in the US: in 2012 the fleet was unused for 63 per cent of the time. This was due to a lack of budgeting for drone operations as well as associated costs for drone maintenance and drone-related equipment. For more recent data, confirming the same problems with the US Drone Border Patrol Program, see Hoffman 2015.
5 *Mare Nostrum* is an operation of a military nature with humanitarian and security purposes, launched by the Ministry of Defence in cooperation with the Ministry of Internal Affairs. It was launched in the aftermath of the Lampedusa disaster of October 2013, in which more than 360 migrants lost their lives in one day. It was in operation until October 2014, and was discontinued due to the high costs involved in the operation financed by Italy and, in the view of the Italian government, the lack of participation by other European states. Recognizing the effort carried out by Italy, the Member States and the EU agreed to replace *Mare Nostrum* with the Frontex coordinated Joint Operation (JO) *Triton*, which nevertheless had a less extended (up to 30 miles from the Italian coast) and a different operational area compared to *Mare Nostrum,* until the disaster of 18 April 2015.
6 An earlier agreement on bilateral cooperation of 28 May 2012 also had as its main goal the training of Libyan authorities, also through operation 'Cyrene'.
7 'Moved to prevent further loss of life at sea and to tackle the root causes of this humanitarian emergency', 'the European Council committed to strengthening the Union's presence at sea, to preventing illegal migration flows and to reinforcing internal solidarity and responsibility' (CD, recital 2).
8 Personal data are defined as 'any information relating to an identified or identifiable natural person', according to the DPD.
9 Visual data are personal data, as stated by the European Court of Human Rights in *Peck v. UK*, Application No. 44647/98, judgment of 28.1.2003, para. 59.
10 Court of Justice (Grand Chamber), Judgment of 8 April 2014, Joint Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd* v. *Ireland*, nyr.
11 Court of Justice (Grand Chamber), Judgment of 6 October 2015, C-362/14 *Maximillian Schrems* v. *Data Protection Commissioner*, nyr.
12 Recital 13 of the Preamble, EUROSUR Regulation.

References

Alston, P. (2010) 'Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions', available at www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf (last accessed 13 August 2015).

Amnesty International (2014) 'Amnesty International's Submission to the Council of Europe Committee of Ministers: Hirsi Jamaa and Others v. Italy (Application No. 27765/09)', available at www.amnesty.eu/content/assets/Doc2014/B1525_-_second_submission_Hirsi_-_11_Feb_2014.pdf (last accessed 2 May 2016).

Art. 29 Data Protection Working Party (2015) 'Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones', 01673/15/EN WP 231, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf (last accessed 2 May 2016).

Balzacq, T. (2008) 'The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Politics', *Journal of Common Market Studies*, 46(1): 75–100.

Bigo, D. (2000) 'When Two Become One: Internal and External Securitizations in Europe', in M. Kelstrup and M.C. Williams (eds), *International Relations Theory and the Politics of European Integration: Power, Security and Community,* London: Routledge.

Council Decision (CFSP) 2015/972 of 22 June 2015 on a European Union Military Operation in the southern Central Mediterranean (EUNAVFOR MED), *Official Journal of the European Union L* 157, 23 June 2015, p. 51, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015D0972 (last accessed 14 November 2016).

Council Framework Decision 2008/977/JHA of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal matters, *Official Journal of the European Union L* 350, 30 December 2008, 60–71.

Custers, B. (ed.) (2016) *The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives*, The Hague; TMC Asser Press.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal data and on the Free Movement of Such Data, *Official Journal of the European Communities L* 281, 23 November 1995, 31–50, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 (last accessed 14 November 2016).

European Commission (2008) 'Examining the creation of a European Border Surveillance System (EUROSUR)'. COM(2008) 68 final, 13.2.2008, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52008DC0068&from=EN (last accessed 2 June 2015).

European Commission (2011) Proposal for a Regulation of the European Parliament and the Council establishing a European Border Surveillance System (EUROSUR), COM(2011) 873 final, available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/eurosur_final.pdf (last accessed 30 July 2014).

European Commission (2012a) Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the free Movement of Such Data (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=en (last accessed 2 May 2016).

European Commission (2012b) Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, COM(2012) 10 final, 25.1.2012, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=en (last accessed 2 May 2016).

European Commission (2013a) Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to Register Entry and Exit Data of Third Country Nationals Crossing the External Borders of the Member States of the European Union, COM(2013) 95 final, 28.2.2013, available at: http://ec.europa.eu/dgs/home-affairs/doc_centre/borders/docs/1_en_act_part1_v12.pdf (last accessed 29 April 2016).

European Commission (2013b) Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Program, COM(2013) 97 final, 28.2013, available at: http://ec.europa.eu/dgs/home-affairs/doc_centre/borders/docs/1_en_act_part1_v14.pdf (last accessed 29 April 2016).

European Commission (2013c) 'EUROSUR: Protecting the Schengen External Borders Protecting Migrants' Lives', available at: http://europa.eu/rapid/press-release_MEMO-13-1070_en.htm (last accessed 10 September 2014).

European External Action Service (2016) 'EUNAVFOR MED Op SOPHIA – Six Monthly Report 22 June–31 December 2015', available at: https://wikileaks.org/eu-military-refugees/EEAS/EEAS-2016-126.pdf (last accessed 2 May 2016).

Finn, R., Wright, D., Jacques, L. and De Hert, P., (2014) Study on Privacy, Data Protection and Ethical Risks in Civil RPAS Operations. Final Report. Publications Office of the European Union, available at: http://ec.europa.eu/DocsRoom/documents/8550 (last accessed 20 April 2016).

Frontex (2014) *Border Surveillance*, available at: http://frontex.europa.eu/research/border-surveillance (last accessed 23 April 2015).

Gertler, J. (2012) 'U.S. Unmanned Aerial Systems', Washington, DC: Congressional Research Service, available at: www.fas.org/sgp/crs/natsec/R42136.pdf (last accessed 2 May 2016).

Guild, E., Carrera, S., and Geyer, F. (2008) 'The Commission's New Border Package: Does It Take Us One Step Closer to a "Cyber Fortress Europe"?', CEPS Policy Brief No. 154, available at: www.ceps.eu. (last accessed 10 June 2015).

Haddal, C.C. and Gertler, J. (2010) 'Homeland Security: Unmanned Aerial Vehicles and Border Surveillance', Washington, DC: Congressional Research Service, available at: www.fas.org/sgp/crs/homesec/RS21698.pdf (last accessed 2 May 2016).

Hayes, B., Jones, C. and Toepfer, E. (2014) *Eurodrones, Inc.* Amsterdam: Transnational Institute, London: Statewatch, available at: www.statewatch.org/news/2014/feb/sw-tni-eurodrones-inc-feb-2014.pdf (accessed 29 April 2016).

Human Rights Watch (2012) 'Losing Humanity. The Case against Killer Robots', available at: www.hrw.org/sites/default/files/reports/arms1112ForUpload_0_0.pdf (last accessed 5 February 2016).

van Lieshout, M., Friedewald, M., Wright, D., Gutwirth, S. (2013) 'Reconciling Privacy and Security', *Innovation: The European Journal of Social Science Research*, 26(1–2): 119–132.

Marin, L. (2011) 'Is Europe Turning into a "Technological Fortress"? Innovation and Technology for the Management of EU's External Borders. Reflections on Frontex and EUROSUR', in M.A. Heldeweg and E. Kica (eds), *Regulating Technological Innovation: Legal and Economic Regulation of Technological Innovation*, Basingstoke: Palgrave Macmillan, 131–151.

Marin, L. (2016a) 'The Humanitarian Drone and the Borders. Unravelling the Rationales Underlying the Deployment of Drones in Border Surveillance', in B. Custers (ed.) *The Future of Drone Use*, TMC Asser Press.

Marin, L. (2016b) 'The "Metamorphosis" of the Drone: Challenges Arising from the Deployment of Drone Technology in Border Surveillance. An Exploratory Study', in D. Bowman, E. Stokes and A. Rip (eds) *Embedding and Governing New Technologies: A Regulatory, Ethical and Societal Perspective*, Singapore: Pan Stanford Publishing.

Marin, L. and Krajčíková, K. (2016) 'Deploying Drones in Policing European Borders: Constraints and Challenges for Data Protection and Human Rights', in A. Završnik (ed.), *Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance*, New York: Springer.

Milivojevic, S. (2016) 'Re-bordering the Peripheral Global North and Global South: Game of Drones, Immobilising Mobile Bodies and Decentring Perspectives on Drones in Border Policing', in A. Završnik (ed.), *Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance*, New York: Springer.

Nolin, P. C. (2012) *Unmanned Aerial Vehicles: Opportunities and Challenges for the Alliance. Special Report*. Canada: NATO Parliamentary Assembly.

Regulation (EU) No. 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur), *Official Journal of the European Union L 295* (6 November 2013), 11–26, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R1052 (last accessed 14 November 2016).

Rosén, F. (2013) 'Extremely Stealthy and Incredibly Close: Drones, Control and Legal Responsibility', *Journal of Conflict & Security Law*, 19(1): 113–131.

Sandvik, K.B. (2016) 'The Political and Moral Economies of Dual Technology Transfers: Arming Police Drones', in A. Završnik (ed.), *Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance*, New York: Springer.

Weaver, O. (1995) 'Securitization and Desecuritization', in R. Lipschutz (ed.) *On Security*, New York: Columbia University Press, 46–86.

Završnik, A. (ed.) (2016) *Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance*, New York: Springer.