When 'digital borders' meet 'surveilled geographical borders'. Why the future of EU border management is a problem

Gloria González Fuster & Serge Gutwirth[1]
Law, Science, Technology and Society (LSTS)
Vrije Universiteit Brussel (VUB)

Intro

Over the last decades, the European Union (EU) has been developing its external 'borders' through a double axis. Firstly, it has encouraged the creation of EU-wide databases that, because they primarily target the movements of third-country nationals, have come to be known as the 'digital borders' of the EU – in contrast to its 'physical borders'. Secondly, the EU has vigorously supported the deployment of technology to monitor the movements towards and at such 'physical borders' of its territory, and transformed them into heavily surveilled zones. Until now, these two trends appeared to progress autonomously, the former revolving around *who* is (or needs, or wishes to be) on European territory, and thus focusing on the processing of what EU law designates as 'personal data' (i.e., 'any information related to an identified or identifiable natural person')[2], and the latter concentrating on *what* happens at and near European frontiers, privileging the treatment of information regarded as non-'personal data' (i.e., which cannot be related to an identified or identifiable person). But the most recent initiatives discussed by EU institutions in relation with border management seem to announce an extremely problematic conflation of approaches.

The construction of 'digital borders'

The origins of the current proliferation of large-scale information systems processing personal data of third-country nationals[3] in the European Union (EU) can arguably be traced back to the establishment of the Schengen area, as created by the Schengen Agreement of 1985,[4] and

[1] Gloria González Fuster is a researcher at the Law, Science, Technology and Society (LSTS) Research Group of the Faculty of Law and Criminology of the Vrije Universiteit Brussel (VUB). Email: Gloria.Gonzalez.Fuster@vub.ac.be. Serge Gutwirth is the director of the Law, Science, Technology and Society (LSTS) Research Group of the Faculty of Law and Criminology of the Vrije Universiteit Brussel (VUB), where he is also professor of law and holder of a research fellowship in the framework of the VUB-Research Contingent. Email: Serge.Gutwirth@vub.ac.be

[2] As defined in Art. 2(a) of Directive 95/46/EC (Directive 95/46/EC of the European Parliament and 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, OJ L 281, 23.11.1995, pp. 31-50) (hereafter, the 'Data Protection Directive').

[3] Legally, the definition of 'third-country national' is dependent on its context, its narrower meaning excluding from its content both EU citizens and nationals of third countries who enjoy the rights of free movement under the agreements between the EU and these third countries (Brouwer, 2008: 8).

[4] Schengen cooperation was incorporated into the EU legal framework by the Treaty of Amsterdam of 1997 (see: *The Schengen* Acquis - *Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders*, OJ L 239, 22.9.2000, pp. 19–62).

as developed by the Schengen Convention of 1990.[5] The Schengen area aimed at being a space where the 'free movement of persons' was to be guaranteed. In order to attain this objective, a series of sub-objectives were defined: the abolishment of checks on persons at the internal borders of the EU, the application of common rules with regard to visas for short stays, as well as with regard to asylum requests and controls at external borders,[6] and the stepping up of cooperation and coordination between national police services and judicial authorities to 'improve security' within the Schengen area.

As *the* key tool to facilitate these developments, an information system was designed: the Schengen Information System (SIS). Its creation was portrayed as a compensatory measure to counterbalance the lifting of controls at the internal borders of the EU. The SIS stores information on objects[7] and persons, and it is predominantly used to save alerts issued by the Member States on third country nationals 'not wanted' inside the Schengen area, so they can be refused entry if necessary. Nowadays, the SIS can be accessed by the police, by border control, customs and judicial authorities, by Europol (the European Law Enforcement Agency), by Eurojust (the EU body responsible for the coordination and cooperation between judicial authorities) and by immigration authorities and consular posts.[8]

Over the years, other information systems have been put in place in relation to different Schengen-related sub-objectives. In the context of the application of common rules concerning asylum requests, the Eurodac database was created.[9] This centralised automated fingerprint identification system functions since 2003[10] and stores fingerprints of all persons aged more than 14 who have applied for asylum in a Member State, as well as people apprehended while unlawfully crossing the Schengen external borders. Officially, the main purpose of Eurodac is to discourage 'asylum shopping'; in other terms, it aims to dissuade asylum seekers from moving around inside the Schengen area. Additionally, national authorities can also compare against Eurodac the fingerprints of third country nationals found 'illegally' on their territory.

In relation to the use of common rules for visas, the Visa Information System (VIS)[11] was conceived. This not yet operational database[12] is to store biometric data on all third-country nationals subject to the EU visa requirement. The VIS aims to prevent 'visa-shopping', which means that it is not only intended to have an impact before the external borders of the Schengen area are reached (inherent to all visa policies), but also to divert individuals from moving from one place to another for the sake of lodging multiple visa requests. VIS will be accessible to asylum, immigration and border control authorities.

---

[5] At present, there are 22 EU Member States are part of the Schengen area, together with Iceland, Norway, Switzerland and Liechenstein.

[6] Although the handling of border matters remains a prerogative of the Member States.

[7] Such as vehicles, firearms, or documents.

[8] See: Council Regulation (EC) No 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, in particular in the fight against terrorism; and Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, in particular in the fight against terrorism. The United Kingdom and Ireland participate in the police cooperation aspects of the SIS, with the exception of alerts relating to third-country nationals on the entry ban list.

[9] Eurodac was conceived in the context of the application of the Dublin Convention, later replaced by Regulation (EC) N° 343/2003 of 18 February 2003 and Commission Regulation (EC) N° 1560/2003 of 2 September 2003, which aim at determining the State responsible for examining the asylum application. It was created by Regulation (EC) No. 2725/2000 concerning the establishment of Eurodac for the comparison on fingerprints for the effective application of the Dublin Convention of 11 December 2002, OJ L 316 as completed by Council Regulation (EC) No 407/2002 of 28 February 2002.

[10] In the then EU-15 Member States, except Denmark, and in Norway and Iceland.

[11] Council Decision 2004/512(EC) establishing the Visa Information System (VIS), OJ L 213/05, 15.6.2004; Regulation (EC) 767/2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 2008 218/60.

[12] The VIS should complete its testing phase at the end of 2010.

EU institutions are currently considering the creation of more large-scale information systems to store biometric data of third-country nationals, and in particular of a so-called 'Entry/Exist System' (EES),[13] which is expected to record the time and place of entry, as well of length of authorised stay, of all third-country nationals entering the Schengen area, and which would transmit automated alerts to 'competent authorities' identifying individuals as 'overstayers' as soon as the time of their authorised stay has elapsed, with the purpose of immigration control. Additionally, the European Commission also suggested that could be developed an Electronic System of Travel Authorisation (ESTA), in order to collect data on third-country nationals not subject to visa requirements prior to their arrival at EU borders.[14]

These 'digital borders' have spread horizontally over the EU following modus and dynamics of *identification.* They are devoted to the processing of data on *whoever* happens to fall in anyone of the categories targeted. Therefore, the data processed in this context generally unequivocally fall under the legal notion of 'personal data' (as they refer to a particular person), and this triggers the application of legal provisions implementing the right to the protection of personal data, a right which has very recently acquired the status of 'autonomous fundamental right' in the EU.[15]

Processing (more) data for security purposes

The setting up of these 'digital borders' has occurred in parallel to the adoption of other measures similarly based on the processing of 'personal data', but (more) directly pursuing security-related objectives, such as counter-terrorism or the fight against serious crime, which were strongly prioritized in the EU after the events of 2001 in New York, and the bombings in Madrid in 2004 and London in 2005. (Personal) data processing measures supported in the last years by EU institutions can imply the increased storage of data,[16] the intensification of data sharing and the making available of data across the internal borders of the EU[17] or across its external borders,[18] or the collection of data on individuals at the borders and its automatic transfer to law enforcement authorities, including across the EU's external borders.[19]

---

[13] See: European Commission (2005:9); European Commission (2006:6); European Commission (2008:7). A legislative proposal is expected in 2011.

[14] European Commission (2008:5).

[15] The right is listed in the Charter of Fundamental Rights of the European Union (OJ C 83/389, 30.3.2010). The Charter had been signed and proclaimed by the Presidents of the European Parliament, the Council and the European Commission At the meeting of the European Council of 7 December 2000, in Nice; it is now binding, by virtue of Art. 6 TEU (as revised by the Treaty of Lisbon). Art. 8 of the Charter, under the heading "Protection of personal data", it establishes the following: *"(1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority."*

[16] For instance, the EU has backed up the recording by communication service providers of all data related to telephone and electronic communications, for a minimum period of six months, during which they shall be available to national authorities for the purpose of the investigation, detection and prosecution of serious crime (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, pp. 54-63).

[17] For example, the sharing of information and criminal intelligence for criminal investigations and criminal intelligence operations has been streamlined through the 'Swedish initiative' (Council Framework Decision 2006/960/JHA, OJ L 386, 29.12.2006, p. 89).

[18] For instance, allowing transfers of data on financial transactions occurring in the EU to the authorities of the United States (US), in the context of the US programme called the Terrorist Finance Tracking Program (TFTP).

[19] Detailed data (known as Advance Passenger Information (API) data) of passengers travelling to the EU from third countries can be communicated by application of a legal instrument adopted in 2004 in the context of border control and the fight against irregular migration (Directive regulating the transmission of Advance Passenger Information (API) by air carriers to border control authorities (Directive 2004/82/EC, OJ L 261, 6.8.2004, p. 24); richer sets of data (known as Passenger Name Records (PNR) data) are to be transferred to third countries, for

This prioritization of security among EU policies also had an impact on the EU's 'digital borders'. Some large-scale information systems have redefined, access to their data has been granted to more parties, and the possible uses of such data has been extended. The SIS was redesigned into a new version, SIS II, and, allegedly in the name of needs in the fight against terrorism, it was established that this new version of the system should store biometric data, such as photographs and fingerprints.[20] In 2009, a legal instrument enabled law enforcement authorities to have access to Eurodac for the purpose of preventing and fighting terrorism. VIS is to be used primarily by visa authorities, but access by a number of other authorities in connection with the fight against terrorism is also foreseen.

All in all, this has led to a situation where major EU-wide large-scale centralised information systems do not respect the principle of purpose limitation, which is one of the basic principles of European data protection law, and according to which data should be used for the specified, explicit and legitimate purpose for which they were collected. The European Commission has openly recognised this problem,[21] even though no urgent measure appears to have been planned to solve it. In some cases, the very nature of certain data processing measures appears to be strongly debatable, and is actually openly debated.[22]

EU's 'digital borders' have not been established for the sake of better knowing third country nationals, satisfying the decision makers' curiosity about them[23] or solely documenting their actions, but to have an influence upon people's movements, by refraining them for entering into or leaving the EU, or discouraging them from moving around an area that for others represents the place for 'freedom of movement'. Additionally, however, they have progressively been transformed into hybrid systems used as background information constantly available for other (symbolically charged) purposes.

A converging architecture

The multiplication of EU-supported data processing initiatives and the blurring of objectives attributed to them have been accompanied by a series of attempts to make them converge more intensely, be it under grand *ad-hoc* policy concepts, or be it through minor (but not inconsequential) practical technical and managerial decisions. Efforts of the first type have essentially produced slightly vague notions such as 'interoperability' of systems[24] and

security purposes, by virtue of different international agreements, and EU institutions have already been discussing the possible deployment of an EU system of collection of PNR data, to be used for law enforcement purposes (see: European Commission (2007)). The European Commission is working to present a Passenger Name Record package consisting of a communication on an EU external PNR strategy and a new EU PNR proposal).

[20] Regulation (EC) 1987/2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381/4, 28.12.2006.

[21] European Commission (2010b: 22).

[22] In this sense, for example, the United Kingdom (UK) objected to the official view according to which giving access to VIS to police authorities and to Europol for the purposes of prevention, detection and investigation of terrorist offences and of other serious criminal offences (Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (OJ 2008 L 218, p. 129) may be regarded as 'an act developing the Schengen *acquis* in the sphere of visas', and requested the European Court of Justice to annul the decision that, on the basis of such consideration, has the effect of excluding the UK from such access. See: *Opinion of Advocate General Mengozzi delivered on 24 June 2010, Case C 482/08 United Kingdom of Great Britain and Northern Ireland v Council of the European Union (Exclusion of the United Kingdom from the procedure for adopting a Council decision concerning access, for consultation for police purposes, to the Visa Information System (VIS)).*

[23] Referring to the 'curiosity by states', see: Guild (2010:3).

[24] European Commission (2005b). About this Communication and the dangers linked to the reduction of "interoperability" to a mere technical issue, see: De Hert and Gutwirth (2006).

'availability' of data,[25] or the only more recently explored 'EU Law Enforcement Information Management Strategy'[26] or 'EU Information Exchange Model'.[27]

But concrete advances towards architectural convergence have been sustained. At a technical level, a good illustration can be provided by the European Commission's own secure data communication network, called s-TESTA,[28] on which Eurodac is already running and on which will run both SIS II and VIS, and which happens to be also the network used by contact points established in the context of the Prüm Decision[29] to handle requests for cross-border comparisons of DNA profiles, fingerprints and vehicle registration data, as well as the network relied upon by Eurojust, Europol, and so-called national Financial Intelligence Units (FIUs) for their own secure communications, and the network that will use the European Criminal Records Information System (ECRIS), a decentralised information system interconnecting Member States' criminal record databases which is currently being established. In the field of biometrics, the development of VIS was explicitly linked to the creation of a Biometric Matching System (BMS) designed to become "*the central biometric component of a collection of European Union identity programs for the protection of citizens and Schengen borders*".[30]

Also at a managerial level, the establishment of an Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, is the pipeline.[31] It is expected to take care of the operational management of SIS II, VIS and Eurodac, and any other future IT system in the area of freedom, security and justice. This has been interpreted as a *de facto* step towards the 'interoperability' of such systems.[32] And in practice, indeed, these developments do create the circumstances that facilitate seamless data flows between any existing and upcoming information systems, and this despite the lack of transparent and accountable decisions pushing in this direction, or any detailed consideration of the problems that this implies in relation to fundamental rights.

'Interoperabilty', 'convergence' and 'availabilty'

In its 2010 panoramic review of information management in the area of freedom, security and justice, the European Commission asserted that putting in place *"a single, overarching EU information system with multiple purposes"* in this area would *"constitute a gross and illegitimate restriction of individuals' right to privacy and data protection"*,[33] and celebrated that no EU information system with such characteristics is in place at the moment. The absence of such a single, overarching EU information system with multiple purposes does not mean, however, that current developments do not constitute already illegitimate restrictions of individuals' right to privacy and data protection.

---

[25] European Commission (2005a). See also the critical comments of the European Data Protection Supervisor (2006:8).
[26] Discussed at Council level in 2009 (European Data Protection Supervisor (2009:12).
[27] The Stockholm Programme: An open and secure Europe serving and protecting citizens, Council Document 5731/10, 3.3.2010, Section 4.2.2.
[28] S-TESTA stands for Secure Trans-European Services for Telematics between Administrations (European Commission (2010b:6)).
[29] Which builds upon an agreement concluded in 2005 by Germany, France, Spain, the Benelux states and Austria to step up cooperation in the fight against terrorism, cross-border crime and irregular migration.
[30] Accenture Press Release (2008), "*Accenture and Sagem Défense Sécurité Win Prime Contract for European Commission's Biometric Matching System*", October 20, available at: http://newsroom.accenture.com/article_display.cfm?article_id=4762
[31] European Commission (2010a).
[32] Bertozzi (2008:25).
[33] European Commission (2010b:3). The fear in face of the introduction of centralised and computerised population databases, already in the late 1970's e.g. in the Netherlands and Germany, was one of the factors that triggered the reactions that eventually lead to the creation of European data protection law (Bennett, (1992:46); Gutwirth (2002:17 et seq.)).

Of course, such restrictions can also occur *irrespective of* the existence of any centralised system. Merely storing and retaining certain types of data in databases that are to be used for criminal identification, for instance, is in itself problematic from a human rights perspective;[34] as it is problematic to use for law enforcement purposes any data that was not collected for such purposes, especially when those whose data is processed are treated as a suspect category.[35] The processing of personal data, in any case, must always go hand in hand with the respect and implementation of detailed data protection provisions, actualising the now fundamental right to the protection of personal data. However, applicable data protection rules are not uniform in the EU legal framework,[36] and this can lead to situations in which the level of protection is unsatisfactorily guaranteed. Moreover, even when the highest level of protection is supposed to apply, satisfactory enforcement can remain a challenge.[37]

But more importantly, it must also be stressed that, due to the way in which large-scale information systems are being developed and managed, their deployment, even if undertaken in a formally decentralised, dispersed way, can have an effect on the fundamental rights on the individual which is fully equivalent to the deployment of a '*a single, overarching EU information system with multiple purposes'*. As soon as such systems are *networked,* they are as a matter of fact transformed into interlinked elements of a single matrix, to be eventually questioned from many different entry zones. Nodal points transfiguring dispersed systems into a network can be EU agencies to which heterogeneous data flows converge and from which they are redirected towards other recipients, or human beings in whose hands intersect multiple access rights, such as 'body guards' or any other 'competent authorities' that EU law often mentions and rarely describes in concrete terms, but that, more often than imagined, happen to be members of the police.[38]

A denial of data protection's cornerstone, the purpose specification principle

All in all, the border-related developments occurring in the name of "availability of data" and the "interoperability" or "convergence" of systems the processing of personal data are obviously contradictory to the purpose specification principle of data protection law. Indeed, the plan to establish an Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, be it as *one* overarching information system or a decentralised organisation of intertwined systems, feeds the legitimate fear that such erosion of the purpose specification principle brings about. This is all the more alarming since the

[34] *S. and Marper v. The United Kingdom*, European Court of Human Rights, Applications nos. 30562/04 and 30566/04, Judgement of 4 December 2008. See also: De Beer de Laer, De Hert, González Fuster and Gutwirth (2010).
[35] Ahumada-Jaidi, A. (2009:2). See also: González Fuster, De Hert, Ellyne and Gutwirth (2010).
[36] Nor specifically in the area of freedom, security and justice, partly due to the fact that before the entry into force of the Treaty of Lisbon in December 2009, said area was split between the first pillar (Title IV) of the EC Treaty, "Visas, Asylum, Immigration and other policies related to free movement of persons") and the third pillar (Title VI of the Treaty on European Union (TEU), Police and Judicial Cooperation in Criminal Matters), allowing for a heavily contrasted development of legislation (see, notably: De Hert, Papakonstantinou and Riehle (2008); and De Hert and Papakonstantinou (2009)). The legacy of this period has still strong implications on EU's data protection (see: Hijmans and Scirocco (2009)).
[37] For instance, in the context of Eurodac, see: Eurodac Supervision Coordination Group (2009). See, for work carried out in relation to SIS: Council of the European Union (2010), *Note from the Drafting Group for Schengen Catalogue on Data Protection to Schengen Evaluation Working Party on Catalogue of recommendations for the correct application of the Schengen acquis and best practices: data protection*, 10 May, Brussels. A particularly telling illustration of the slowness of 'progress' in this area is the 'information sharing practices' among national data protection authorities, or, more precisely, their absolute non-existence. Despite the impressive support granted by EU institutions to information technology, in general, and data processing, in particular, when a the data protection authority of a Member State considers that it is not competent to deal with a particular complaint, and interprets that the case should be treated by the data protection authority of another Member State, said authority can still decide, in 2010, and in full compliance with its legal obligations, to *send a letter* to the other authority (see, for instance, the Resolution R/00851/2010 of 13/04/2010, for procedure TD/00314/2010, of the Agencia Española de Protección de Datos (AEPD)).
[38] Carrera (2010: 9).

purpose specification principle is the core principle of data protection law,[39] and more specifically of the Data Protection Directive.[40] The underlying rationale of data protection goes as follows: the processing of personal data is not banned, but it is (except for some categories of sensitive data) in principle allowed on the condition that the processing is limited to meet specified, explicit and legitimate purposes.[41] Implicitly, the old constitutional idea of the separation of powers is at work again: to keep the power of data processors in check, different data processing activities must be and remain unconnected, and such is what the purpose specification principle warrants. In other words, the processing of personal data is not prohibited, but each processing of personal data has to be (kept) separate. And that turns the purpose of the processing into the most important touchstone of data protection law, since it provides the criteria to judge the legitimacy of processing, the quality of the data and the way they are used. That is even the case when the 'data subject' gave his/her consent.

In other words, data protection law stands of falls with the ex ante explicit and specific delineation of the legitimate purpose of the processing and its subsequent respect in terms of data collected and their use. From that point of view, "catch all" purposes threaten to undermine the whole legislative framework and must be considered illegitimate, just as is the case for the merging, bridging and linking of initially separated processings with a different goal. This makes the evolutions we described above all the more worrisome and threatening. The developed practices and plans to 'interoperationalise' the existing (and not yet existing or not yet operational) informational devices with specific and explicit goals in the name of underdetermined purposes that are amalgamating crime-fighting, "war against terrorism", security, migration, visa policies, border control, border surveillance, asylum, the "movement" of non-EU-nationals in the EU, and more, to one vague and non-explicit purpose, do not so much represent an occasional friction or marginal conflict relating to data protection law, but embody a more fundamental rejection of its rationale. In other words, the initiatives and plans we described symbolise the negation of the core of the new fundamental right to data protection. As a matter of fact, "interoperability" and "the principle of availabilty" are data protection's anti-principles.

Against this background, and regardless of repeated references by EU's policy documents to concepts such as '*privacy-by-design'*,[42] the current evolution can only be qualified as a progressive embedding into the EU's area of freedom, security and justice of an '*impossibility-of-privacy-by-design'*, as it substantiates in the circumstances that surround the functioning of large-scale information systems the conditions that violate fundamental legal principles such as the already mentioned purpose limitation principle. Yet, the most worrisome evolution is only now starting to be visible. It concerns the connexion of the 'digital borders' processing devices of the EU, which have been progressively networked in

39 Gutwirth (1993). Also: Gutwirth (2002:96 et seq).

40 Cf. Art. 6 of the Data Protection Directive: "1. Member States shall provide that personal data must be: (a) processed fairly and lawfully; (b) *collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use; 2. It shall be for the controller to ensure that paragraph 1 is complied with."

41 That is why we described data protection law as an example of legal tool that fosters 'transparency', controllability and accountability of the powerful actor (in contrast to 'opacity'-tools that protect individuals by shielding them off from powerful actors as the state by prohibitions to interfere with their freedom or autonomy (such as privacy protection). See: De Hert and Gutwirth (2006).

42 And related notions, such as 'Privacy Enhancing Technologies' (PETs) (see, notably: European Commission (2007a)).

this troublesome fashion, to the tools used in the area of border surveillance and border control.

A new turn: the coupling with surveillance at the geographical borders (Frontex and Eurosur)

EU border management has been mutating over the last years, under the strong influence of the security discourse that permeated all Schengen-related priorities, and shaped by heavy reliance on technological 'solutions'.[43] Two names encapsulate these developments: Eurosur and Frontex. Eurosur is a European border surveillance technical framework conceived with to improve 'border security' through data exchange and coordination of activities,[44] designed to support the Member States' efforts in this field. It saw the light in the context of EU's interest on the protection of its maritime borders through the deployment of technical systems. Frontex is the European Agency for the Management of Operational Cooperation at the External Borders, created in 2005[45] to coordinate (external) border-control surveillance operations. It is dedicated to the application of the EU common corpus of legislation on borders,[46] and also has as core tasks risk analysis and risk assessment.

Until recently, developments taking place in relation with the EU's external borders appeared to be exclusively concerned with dynamics of *detection*, the aim being to discern events taking place at the borders or near them, but not to identify particular people. This is the domain of satellites, sensors, cameras, flying devices. Frontex, notably, was originally not granted the possibility to process any 'personal data', and appeared not to require such ability in order to fulfil its allocated tasks.

A revision of Frontex's mandate is currently being negotiated. The new tasks proposed for Frontex by the European Commission include the widening of its work related to risk analysis, the coordination of joint return operations, a series of tasks related to the development and operation of information systems and a series of tasks related to providing assistance to Eurosur.[47] In the light of these discussions, the European Data Protection Supervisor (EDPS) has pointed out that one is entitled to consider that Frontex will presumably have to process data that appears to fall under the legal category of 'personal data', and has called for open recognition of this fact and subsequent compliance with data protection obligations.

Nevertheless, a major coupling of the 'digital borders' of the EU and these (external) border surveillance practices is starting to materialise through a channel that is substantively different from the mere addition of Frontex or Eurosur to the long list of European bodies entrusted to process 'personal data'. Such channel is being build up through the reliance on '*intelligent*' or 'smart' surveillance techniques.[48]

These techniques are sometimes referred to as 'data mining' or 'profiling', are based on ambient intelligence practices, and rely on the massive processing of data in order to identify *patterns* that allow for the automatic categorisation of information. In practice, these

[43] Particularly present in the 2008 Communication of the European Commission, already mentioned (Hobbing, 2010:69).
[44] See: European Commission (2008a).
[45] Frontex is an agency created by the Council Resolution No. 2007/2005/EC establishing a European Border Agency on 1 May 2005 in Warsaw.
[46] The Schengen Borders Code (*Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders*, Official Journal L 105, 13/04/2006, pp. 1-32).
[47] European Data Protection Supervisor (2010:3).
[48] Wright, Friedewald, Gutwirth, Langheinrich, Mordini, Bellanova, De Hert, Wadhwa and Bigo (2010).

techniques involve on the processing of very different types of data (behavioural biometrics, cyberspace information, data collected through satellite, etc.) and aim at a sort of automated discrimination of responses, or what is euphemistically designated by the industry that sells these services as 'intelligent filters'[49] for 'smart borders'.[50] The EU is generously funding research to apply these kind of techniques to border surveillance, and the European Commission tends to accept them as unproblematic it in its policy documents.[51]

However, law and, more particularly, data protection law, has been struggling to deal satisfactorily with these techniques and practices, since they often 'walk' on the thin line that separates the application of data protection law from its non-application.[52] Since the changer between both options is triggered by the presence or not of the processing of 'personal data' and the contours of the legal definition of such 'personal data' are contested, the efficient application of data protection seems very doubtful.

Concluding remarks: from data protection back to the right to privacy

As the information systems that were supposed to replace (internal) border control meet the new technologies deployed to reinforce (external) border control, the borders of Europe increasingly look as invisible ever-growing walls whose shadows darken an ever-expanding space. Next to the important political and ethical discussions about the political desirability and acceptability of the construction of such 'fortress Europe' and about the implicit stigmatisation of 'people on the move' and 'movements' across the external borders of the EU, the gradual entangling of the digital borders-devices and the surveillance of geographical borders that we shortly summarised rise fundamental legal issues that are not limited to issues of personal data. They concern, notably, the right to privacy.[53]

As already pointed out, the right to the protection of personal data has only very recently been recognised as a separate fundamental right in the EU legal framework. In the context of the Council of Europe, which represents the chief reference for the EU in the area of human rights, the protection of personal data has never reached such a status: it is traditionally granted by the European Court of Human Rights under the umbrella of the right to respect for private life – not as constituting an autonomous right in itself. The EU has privileged the separate treatment of data protection, *inter alia,* by adopting detailed *ad-hoc* legislation and by putting in place several institutional actors exclusively dedicated to the monitoring the protection of personal data ('data protection authorities' such as the EDPS). But this progressive emancipation of the right to the protection of personal data in the EU framework has come at a price, which is the correlated sidelining of issues related to the right to respect for private life.

As enshrined in Article 8 of the European Convention on Human Rights (ECHR),[54] the right to respect for private life is ultimately concerned with the protection of individuality, personal

[49] Hjelmstad, Jensen and Vagran (2010: 4).
[50] *Ibidem*, p. 9.
[51] The European Commission has declared that the development of risk profiles '*is relevant'* for the purpose of identifying security threats (European Commission (2010b:26). It is very unclear what is considered 'risk', as a practical example of "*risks successfully managed*" that is given consists in preventing a person form applying for asylum in several Member States (idem).
[52] See, notably: Bygrave, Lee A. (2001); Hildebrandt and Gutwirth (2008: particularly the chapters 13 and 14); Dinant, Lazaro, Poullet, Lefever and Rouvroy (2008); González Fuster, Gutwirth and Ellyne (2010); and Wright, Friedewald, Gutwirth, Langheinrich, Mordini, Bellanova, De Hert, Wadhwa and Bigo (2010).
[53] In fact those issues do also concern the fundamental principles of criminal law as they are mentioned in Art. 6 of the European Convention on Human Rights on the right to a fair trial, notably the presumption of innocence and the *nullum crimen, nullum poena, sine lege* rule. This, however, is not the subject of the present chapter.
[54] European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, 213 U.N.T.S. 222, as amended by Protocol No. 11.

autonomy and self-determination – in a word, of freedom. Although entangled in the rich node of signification embodied by the word '*private*', and thus often misconceived, the right to respect for private life of Article 8 ECHR (that the EU legal framework systematically designates as 'the right to privacy') is not about the *secret*, *hidden, intimate* or *non-public* life of individuals, but with their *own* life; it is not about what strict conceptions of privacy, particularly common in Anglo-American usage, reduce to a residual space free of physical interference, far from prying eyes, or a place 'to be left alone'; and it is absolutely indifferent to any definition or redefinition of the *public v. private* dichotomy, because it encompasses both the former and the later.

The right to respect for private life is profoundly affected by the described developments in relation with borders. And its careful consideration becomes crucial when data processing practices develop through the interstices of data protection law, for instance as they (try to) escape regulation by disputing the qualification of the data processed as 'personal data'. As soon as practices are put in place with the aim either to steer or influence individual conduct or to manage/control streams of people, be it 'identified' or 'unidentifiable' individuals or people, the issues at stake might well not resort under data protection, but they still are related to the respect for private life – because issues of freedom are at stake too. If the right to personal data protection appears to be singularly fit to ensure the protection of individuals in face of border policies focusing on *who* is on the move (and/or is not moving in the desired direction), it is, in its current form, dramatically ill-suited as an effective response to the negative effects of initiatives formally directed towards the detection of *whatever* happens at borders, or mixing and blurring both approaches. Moreover, where data protection law by default regulates –and thus conditionally accepts and enables– the processing of personal data, the respect of private life and the autonomy of the individual it protects, is by default prohibitive and normative.[55] A return to the right to respect for private life seems thus urgently needed in order to better understand, and react to, the most troubling developments taking place in relation with EU border management.[56]

List of references:

Ahumada-Jaidi, A., 2009. *Border control and internal security in the European Union – information, technology and human rights implications for third-country nationals 14.1 (Legal analysis of pre-entry screening measures)*. DETECTER (Detection Technologies, Terrorism, Ethics and Human Rights) Project.

Bennett, C.J., 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca and London: Cornell University Press.

Bertozzi, Stefano, 2008. *Schengen: Achievements and Challenges in Managing an Area Encompassing 3.6 million km2*, CEPS Working Document No. 284. Brussels: Centre for European Policy Studies (CEPS).

Brouwer, Evelien, 2008. *Digital borders and real rights: effective remedies for third-country nationals in the Schengen Information System*. Leiden: Martinus Nijhoff Publishers.

---

[55] On the differences between the fundamental right to respect of private life and data protection law, see De Hert and Gutwirth (2006).

[56] In terms of EU legislation this is not a novelty, since Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ L 201, 31.7.2002, pp. 37-47) (known as the 'e-Privacy Directive') already operated such a 'return to privacy' by inventing a protection system for location and traffic data that are not necessarily personal data, but can heavily impact upon individuals' autonomy.

Bygrave, Lee A., 2001. 'Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling', *Computer Law & Security Report* 17:17-24.

Carrera, Sergio, 2010. *Towards a Common European Border Service?*. Brussels: Centre for European Policy Studies (CEPS).

De Beer de Laer, Daniel, Paul De Hert, Gloria González Fuster and Serge Gutwirth, 2010. 'Nouveaux éclairages de la notion de "donnée personnelle" et application audacieuse du critère de proportionnalité, Cour européenne des droits de l'homme, Grande Chambre, *S et Marper C. Royaume Uni*, 4 Décembre 2008', *Revue trimestrielle des droits de l'homme* 81:141-61.

De Hert, Paul and Serge Gutwirth, 2006. 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power', in E. Claes, A. Duff and S. Gutwirth, eds., *Privacy and the criminal law*, Antwerp/Oxford: Intersentia (61-104).

De Hert, Paul and Vagelis Papakonstantinou, 2009. 'The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for', *Computer Law & Security Review,* 25:403-414.

De Hert, Paul, Vagelis Papakonstantinou and Cornelia Riehle, 2008. 'Data protection in the third pillar: cautious pessimism', in M. Martin, ed., *Crime, rights and the EU: The future of police and judicial cooperation*, London: Justice (121-194).

Dinant, Jean-Marc, Christophe Lazaro, Yves Poullet, Nathalie Lefever and Antoinette Rouvroy, 2008. *Application of Convention 108 to the profiling mechanism: Some ideas for the future work of the consultative committee (T-PD)*, Expert report for the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg: Council of Europe.

Eurodac Supervision Coordination Group, 2009. *Second Inspection Report*. 24 June, Brussels.

European Commission, 2005a. *Proposal for a Council Framework Decision on the exchange of information under the principle of availability*, COM(2005) 490 final, 12.10.2005, Brussels.

--- 2005b. *Communication from the Commission to the Council and the European Parliament: On improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs*, COM(2005) 597 final, 24.11.2005, Brussels.

--- 2006. *Communication from the Commission on on Policy priorities in the fight against illegal immigration of third-country nationals,* COM(2006) 402 final, 19.7.2006, Brussels.

--- 2007. *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*. COM(2007) 228 final, 2.5.2007, Brussels.

--- 2007a. *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes,* COM(2007) 654 final, 6.11.2007, Brussels.

--- 2008a. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Examining the*

creation of a European border surveillance system (EUROSUR), COM(2008) 68 final, Brussels.

--- 2008. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Preparing the next steps in border management in the European Union,* COM(2008) 69 final, 13.2.2008, Brussels.

--- 2010a. *Amended Proposal for a Regulation (EU) No ... / ... of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice,* COM(2010) 93 final, 19/03/2010, Brussels.

--- 2010b. *Communication from the Commission to the European Parliament and the Council: Overview of information management in the area of freedom, security and justice,* COM(2010) 385 final, 20.7.2010*,* Brussels.

European Data Protection Supervisor, 2006. *Opinion on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final)*. OJ C 116, 17.05.2006.

--- 2009. *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on an Area of freedom, security and justice serving the citizen*, 10 July, Brussels.

--- 2010. *Opinion on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX).* 17 May, Brussels.

González Fuster, Gloria, Paul de Hert, Erika Ellyne and Serge Gutwirth, 2010. *Huber, Marper and Others: Throwing new light on the shadows of suspicion*. INEX Policy Brief No. 11. Brussels: Centre for European Studies (CEPS).

González Fuster, Gloria, Serge Gutwirth and Erika Ellyne, 2010. *Profiling in the European Union: A high-risk practice*. INEX Policy Brief No. 10. Brussels: Centre for European Studies (CEPS).

Guild, Elspeth, 2010. *Global Data Transfers: The human rights implications*, INEX Policy Brief N° 9, INEX Project.

Gutwirth, Serge. 1993. 'De toepassing van het finaliteitsbeginsel van de Privacywet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens' [The application of the purpose specification principle in the Belgian data protection act of 8 December 1992], *Tijdschrift voor Privaatrecht* 1993/4: 1409-1477.

--- 2002. *Privacy and the information age.* Lanham: Rowman & Littlefield.

Hijmans, Hielke and Alfonso Scirocco, 2009. 'Shortcomings in EU Data Protection in the Third and the Second Pillars: Can the Lisbon Treaty be Expected to Help?'. *Common Market Law Review* 46:1485-1525.

Hildebrandt, Mireille and Serge Gutwirth, eds., 2008. *Profiling the European Citizen: Cross disciplinary perspectives*. Dordrecht: Springer Science.

Hjelmstad, Jens, Erling Jensen and Espen Vagran, 2010. *Intelligent Human Filtering at Europe's External Borders*, INEX Paper, Brussels: INEX Project.

Hobbing, Peter, 2010. 'The management of the EU's external borders : From the Customs Union to Frontex and e-borders', in Guild, Elspeth, Sergio Carrera and Alejandro Eggenschwiler, eds., *The Area of Freedom, Security and Justice Ten Years On: Successes and Future Challenges Under the Stockholm Programme*, Brussels: Centre for European Policy Studies (CEPS).

Wright, David, Michael Friedewald, Serge Gutwirth, Marc Langheinrich, Emilio Mordini, Rocco Bellanova, Paul De Hert, Kush Wadhwa and Didier Bigo, 2010. 'Sorting out smart surveillance', *Computer Law & Security Review*, 26:343-354.