HAL
archives-ouvertes.fr

EUROSUR – A Sci-fi Border Zone Patrolled by Drones?

Daniel Deibler

▶ To cite this version:

Daniel Deibler. EUROSUR – A Sci-fi Border Zone Patrolled by Drones?. Jan Camenisch; Simone Fischer-Hübner; Marit Hansen. Privacy and Identity Management for the Future Internet in the Age of Globalisation: 9th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2, International Summer School, Patras, Greece, September 7–12, 2014, AICT-457, Springer, pp.87-109, 2015, IFIP Advances in Information and Communication Technology (TUTORIAL), 978-3-319-18620-7. <10.1007/978-3-319-18621-4_7>. <hal-01431600>

HAL Id: hal-01431600
https://hal.inria.fr/hal-01431600

Submitted on 11 Jan 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution| 4.0 International License

EUROSUR

A sci-fi border zone patrolled by drones?[1]

Daniel Deibler
Unabhängiges Landeszentrum für Datenschutz, Kiel, Germany

Abstract: In the context of the smart border initiative, the European Union also established a mass surveillance and data exchange programme, called European External Border Surveillance System (EUROSUR). This paper will look at the compliance of the respective European regulation and the implementation of the system with Article 8 ECHR[2] as well as Articles 7 & 8 EUFRCh[3]. This paper will argue that due to the concrete circumstances of the data processing and the large scale of the surveillance, the EUROSUR system constitutes a serious interference with the right to data protection and privacy. While the necessity of such an additional and intrusive border management tool is already highly questionable, in the end, the interference is not justified. In particular, the vagueness in most parts of the regulation and the lack of specific privacy protecting safeguards preclude the fulfilment of the 'quality of law' requirements. Furthermore, it will be shown that a more privacy preserving version is conceivable. As a result, EUROSUR is neither in accordance with law, nor necessary, nor proportionate, and therefore violates Article 8 ECHR as well as Articles 7 & 8 EUFRCh.

Keywords: Privacy, Data Protection, EUROSUR, Surveillance, Border Control, European Convention on Human Rights, Charter of Fundamental Rights of the European Union, European Union, Frontex

> *The EU is going down a very dangerous route of tracking, storing and accessing data on individuals' movements without an adequate grip on the consequences for privacy, notably through 'profiling', misuse and carelessness*.[4]
>
> Baroness Sarah Ludford
> Member of the European Parliament

1 Introduction

In the above quote baroness Ludford was criticising the 'smart border' initiative of the European Commission which was announced in February 2008. This initiative consisted of two proposed instruments to manage the external borders of the European Union (Entry/Exit System, Registered Traveller Programme) and was complemented by a proposal for the creation of a European External Border Surveillance System (EUROSUR). The subsequent criticism from data protection authorities and privacy promoting organisations concentrated mostly on the smart border initiative while the EUROSUR proposal was implemented without any mayor outcry or public discussion. The little expressed criticism for the – in the meantime established – surveillance system came mostly from NGOs in the field of migrant and refugee protection. Organisations such as Pro Asyl[5] or the Jesuit Refugee Service[6] have scrutinised the compliance of EUROSUR with the obligations deriving from the 1951 Geneva Convention relating to the status of refugees as well as other migrant protecting agreements. Consequently this paper sets out to close the existing void and will therefore examine the possible interferences of EUROSUR with the right to privacy and data protection. On the basis of the EUROSUR Regulation[7] the first part of the paper (section 2) will outline the structure and functioning of EUROSUR and describe which information from which sources are imported into the so called 'system of systems'. In addition, the compliance with the rights to privacy and data protection will be examined (section 3). It will be argued that due to the concrete circumstances of the data processing and the large scale of the surveillance, EUROSUR constitutes a serious interference with the right to data protection and privacy (sections 3.1.2 and 3.1.3). In the end this interference is ultimately not justified (section 3.2). In particular, the vagueness in most parts of the regulation and the lack of specific privacy protecting safeguards preclude the fulfilment of the 'quality of law' requirements (section 3.2.1). Furthermore, the necessity of such an additional and intrusive border management tool is highly

questionable and raises concerns in regards to its usefulness (section 3.2.3). Last but not least it will be shown that the interference by the current system and the legislation is greater than necessary, since a more privacy preserving version is conceivable (section 4). As a result, EUROSUR is neither in accordance with law, nor necessary, nor proportionate and therefore violates Article 8 ECHR[8] as well as Articles 7 & 8 EUFRCh[9].

2 EUROSUR – A System of Systems

By establishing a European Border Surveillance System the European Union is attempting to move away from the traditional patrolling of borders to a more risk-based approach to border control. This approach is described in the EUROSUR Regulation as improving the situational awareness and increasing the reaction capability at the external borders.[10] This fairly vague description of EUROSUR and the extent of the surveillance becomes clearer by looking at the definition of 'situational awareness' included in the regulation:

> *'situational awareness' means the ability to monitor, detect, identify, track and understand illegal cross-border activities in order to find reasoned grounds for reaction measures on the basis of combining new information with existing knowledge, (...)*[11]

To achieve this improved situational awareness the regulation establishes a common framework for the exchange of information and for the cooperation between the national authorities responsible for border surveillance as well as Frontex[12]. EUROSUR has been described as a 'system of systems' because it does not establish one centralised database but connects the different so-called National Coordination Centres (NCC) of the participating Member States with each other and Frontex via a communication network which allows:

- information exchange in near-real-time;
- audio and video conferencing;
- handling, storing, transmission and processing of information.

Furthermore, to streamline the information exchange via the National Situational Pictures, the regulation obliges the NCCs to collect the relevant information from a vast array of sources (including national border surveillance systems, liaison officers, border authorities from third countries and ship reporting systems)[13] and to establish and maintain their picture. The Situational Pictures from the different NCCs will be shared which each other and Frontex. Frontex itself, however, will moreover supplement the national information with information from European Union bodies, offices and agencies as well as other undefined sources to create a European Situational Picture, which will subsequently be shared over the network too. Similar sources will be used by Frontex to maintain an additional Common Pre-frontier Intelligence Picture, increasing the knowledge about activities beyond the external borders of the Schengen Area.

The above mentioned range of different sources of information hinders every examination of the information which will be processed in the NCCs. Nevertheless, since the collection of data on a national level as well as the exchange of information between national authorities is regulated by the national law of the Member States, it falls outside the scope of the EUROSUR Regulation and consequently of this paper. However, the data processed in the NCCs is the foundation of the information exchanged in the EUROSUR system and therefore relevant for the Situational Pictures. The regulation itself provides only limited instructions on which information should be included in the Situational Pictures. According to Art. 8 EUROSUR Regulation it consists of an event, an operational and an analysis layer. The event layer shall contain information about incidents regarding unauthorised border crossings, cross border crime and crisis situations. Furthermore the event layer will provide

> *information on unidentified and suspect vehicles, vessels and other craft and persons present at, along or in the proximity of, the external borders of the Member State concerned, as well as any other event which may have a significant impact on the control of the external borders.*[14]

The operational layer will provide information on the position, status and type of border control assets. Last but not least, the analysis layer consists of analysis and risk assessments for the relevant border sections. However, it also includes reference imagery and analysed information relevant for the purpose of the regulation. Beyond

these general descriptions of the exchanged data no concrete information is publicly available. The relevant documents explaining the specifications of the information exchange are not yet available[15], are EU-restricted and government-use-only, or have been presented and discussed in confidential project advisory boards and the EUROSUR Member States' expert group.[16] Nevertheless, presentations by Frontex and the European Commission, such as the infographic EUROSUR[17], allow us to catch a glimpse of the event layer of the European Situational Picture. The included exemplary incident reports of the European Picture show that each event is filed under the location, time, date and type of the incident and illustrated on a map of Europe. Furthermore, each event is described in a free text field (e.g. persons involved, arrests or seizures, additional comments) and the user interface allows attaching images, videos, or other documents as well as to create linkages, or add historical backgrounds. It seems that the National and the Pre-Frontier Situational Picture will also include the above mentioned information since, according to the regulation, they are all structured the same way.

This information exchange will be further complemented by the common application of surveillance tools. According to the regulation ship reporting systems, satellite imagery and any sensors mounted on a vehicle, vessel or craft shall be used to monitor third country ports and coasts, pre-frontier areas and areas in the maritime domain, as well as to track vessels or other crafts in the high seas. Frontex is free to use these surveillance tools on its own initiative and the collected information can also be requested by the NCC of a Member State. For this purpose Frontex shall combine the information from the different sources and analyse the data to create so-called surveillance information on the external borders and on the pre-frontier area.[18]

3 EUROSUR and the Right to Privacy and Data Protection

EUROSUR is in its core a mass-surveillance tool combined with a large-scale exchange of data. Consequently, the activities under the EUROSUR regulation raise questions in regards to its compliance with the fundamental rights of respect for private life and protection of personal data (Art. 7, 8 EUFRCh and Art. 8 ECHR). While the EUFRCh differentiates between the right to privacy – as part of the right to respect for private life – and the right to data protection, both fundamental rights are embraced in the broad term of 'private life' in the ECHR.[19] However, since both rights inter-relate strongly the ECJ[20] favours a joint reading of Art. 7 and 8 EUFRCh and relies heavily on the jurisprudence of the ECtHR[21].[22] Therefore, based on the jurisdiction of the ECJ and the ECtHR, this section will examine if EUROSUR interferes with these fundamental rights.

3.1 Interference with the Right to Privacy

Regarding the legality of surveillance the ECtHR stated in the *Peck case*[23] that

> *the monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life.*[24]

Nonetheless, while the mere act of monitoring will not interfere with one's right, the recording of such data can constitute an interference.[25] Furthermore, the Court decided in the *Amann case*[26] as well as in the *Rotaru case*[27] that the compilation of data by security services on particular individuals can affect the private lives of the victims,[28] even if only public information is systematically collected and stored in files.[29] Consequently, the interference is independent from the way of surveilling[30] – covert or overt – but dependent from the storing and further processing of the data. Besides the fact that data has to be collected, an interference further presupposes that personal data is processed. Therefore, the right to private life in form of the right to privacy and the right to protection of personal data do not just inter-relate in this context but overlap mostly.

3.1.1 Personal Data

In European law personal data is commonly understood as '*any information relating to an identified or identifiable natural person.*'[31]

The element of 'any information' shows the broad concept of personal data and evidently includes images or other data from CCTV, surveillance sensors or other surveillance tools.[32] However, more

problematic is, in the context of surveillance information, the question of whether a person is recognisable or identifiable.[33] This problem will be ascertained in detail below.

The second element requires that the information is relating to someone. However, the concept of 'relating to' is broader than the common understanding of the notion and therefore, data is not only relating to a person if the content of the data is explicitly about this person. According to the Article 29 Working Party, a relationship between data and a specific person can also result from the purpose or the result of the data processing. When data is used "*with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual*"[34] the processed information relates to a specific person. Similarly, data is relating to a person if the use of the information is likely to have an impact on a certain person's rights and interests, however small the impact is.[35] "*It is sufficient if the individual may be treated differently from other persons as a result of the processing of such data.*"[36]

According to the next element of the definition data has to be relating to an identified or identifiable person. While the term 'identified' is self-evident, particular explanations are necessary for the notion of 'identifiability'. In general a person is identifiable if he or she is "*described in the information in a way which makes it possible to find out who the data subject is by conducting further research*."[37] Consequently, it is not necessary to identify a person by finding out his or her name, but it suffices to combine different criteria of personal attributes so that the group, the person belongs to, can be narrowed down and the person can be distinguished from other individuals.[38] Furthermore it is not necessary that the data processor has all the relevant information and significant criteria to identify the individual, since the decision regarding the question if data is personal data is made objectively. Even if only friends or family members can recognise a person on a video due to e.g. his or her figure, haircut and cloth, the data in form of a surveillance tape has to be categorised as personal data.[39] Moreover, the period of data storage becomes relevant in this context. Even if identification is not possible today, data will be personal data if identification becomes possible during the 'lifetime' of the data, due to new information or new technical possibilities. Last but not least, the purpose of the processing also affects the concept of 'identifiability'. In cases where the purpose of the data processing is the identification of specific individuals, the purpose implies that the processor will be able to identify persons and therefore the processed data has to be categorised as personal data again. The Article 29 Working Party explains this concept by the example of video surveillance:

> *As the purpose of video surveillance is, however, to identify the persons to be seen in the video images in all cases where such identification is deemed necessary by the controller, the whole application as such has to be considered as processing data about identifiable persons, even if some persons recorded are not identifiable in practice.*[40]

Consequently, identification is highly dependent on the particular situation and circumstances of the processing, the additional information that is or will be available, and the purpose of the processing. In particular the issue of contextualisation has to be considered regarding depersonalised or statistical data since even if only aggregated data is processed, it might enable the identification of persons if the original sample is too small or additional information is available.

Lastly, the information has to relate to a natural person. Even though the term is self-explanatory, it has to be mentioned that information which seems to relate to objects might also contain personal data. Data about objects such as boats or cars can also contain personal data about the captain or owner of the vessel in question.[41]

3.1.2 EUROSUR and Personal Data

In a next step these general considerations about the concept of personal data have to be applied to the EUROSUR surveillance and data exchange.

Concerning the common application of surveillance tools the European Commission regards the use of modern surveillance technology as a key element of EUROSUR and stated that in particular the fusion of data received from ship reporting systems and satellite imagery plays an essential role.[42] As previously discussed,

the data from vessel monitoring systems may already on its own contain personal data relating to the captain or owner of a vessel.[43] Nevertheless, this personal data is furthermore complemented by satellite imagery or data from any sensor mounted on any vehicle, vessel or other craft.[44] While those sensors might not be designed to identify or track natural persons, the images the system takes when monitoring vessels, beaches or ports will also depict individuals.[45] Depending on weather conditions, light, distance, range, and resolution of photographs the data from the surveillance tools can allow identification of individuals and therefore may constitute personal data. Furthermore, the necessary soft- and hardware already exist to post edit imagery and increase its resolution.[46] While this possibility is less likely when using satellites for monitoring, since they only allow detection of objects larger than 50 cm,[47] the EUROSUR Regulation also permits the use of Remotely Piloted Aircraft Systems (RPASs). Currently the use of Unmanned Aerial Vehicles (UAVs) is prohibited in European civil airspace, however, using Optional Piloted Aircrafts (OPAs) is allowed when someone is on board as an additional safety feature, even if the real pilot is operating the craft from a ground station and Frontex is already interested in acquiring an OPA for the surveillance of external borders.[48] As RPASs can be equipped with different sensors (e.g. high-resolution cameras and microphones or thermal imaging equipment)[49] including some that can zoom into 50 cm they would certainly allow the identification of persons from the high resolution images.[50] The EUROSUR regulation permits the use of such sensors and therefore the processing of such personal data. Furthermore, the regulation obliges Frontex not only to gather this surveillance information but also to supply the NCCs with the information. Consequently, the application of common surveillance tools in the EUROSUR Regulation foresees and permits the processing of personal data and thus, interferes with the right to privacy and protection of personal data.

The second element of EUROSUR, relevant regarding the processing of personal data, is the data exchange via the Situational Pictures (National, European and Pre-Frontier). According to the Commission, EUROSUR does not intend to regulate the storage or cross border exchange of personal data[51] and therefore the "*possibility for exchanging personal data in EUROSUR is very limited: At European level, Member States and Frontex are entitled only to exchange ship identification numbers*."[52] Nevertheless, the limitation to the exchange of ship IDs has only found its way into the regulation regarding the European and the Pre-Frontier Situational Picture.[53] Furthermore, the processing of personal data is envisaged in the regulation in specific circumstances, even if they are described as exceptional.[54] Nonetheless, closer scrutiny reveals that the exchange of personal data was broadly enabled by EUROSUR and might even become the norm. A questionnaire regarding the use of personal data in the NCCs showed that nine NCCs were already processing personal data and one NCC was planning to do so in the future. Furthermore, while only two Member States responded that they were not planning on handling personal data for border surveillance purposes, the rest of the states did not reply to the question.[55] In the context of data exchange and provision of supposedly anonymised data, another statement of the Article 29 Working Party has to be observed:

> *Thus, it is critical to understand that when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data. Only if the data controller would aggregate the data to a level where the individual events are no longer identifiable, the resulting dataset can be qualified as anonymous. For example: if an organisation collects data on individual travel movements, the individual travel patterns at event level would still qualify as personal data for any party, as long as the data controller (or any other party) still has access to the original raw data, even if direct identifiers have been removed from the set provided to third parties.*[56]

Additionally, it has to be noted that the perception of personal data differs between European Member States and that for example the relevant authorities of Spain or Romania do not categorise surveillance images as personal data.[57] Furthermore, the EUROSUR Regulation does neither entail any restrictions on the data exchanged between the NCCs nor does the user interface limit the possibilities of the NCCs.

> *Events uploaded in the system are essentially text boxes where information on persons could be shared. There are no alert pop-ups or other safeguards to ensure that personal data are not inadvertently included or that text boxes are anonymised. Furthermore, EU Member States are also encouraged to*

> *report "information on unidentified and suspect platforms and persons present at or nearby the external borders". The system also allows for video and picture attachments to an event.*[58]

While these considerations concern only the National Situational Picture, it also affects the European and Pre-Frontier ones, since the latter two are based on the information provided from the different NCCs.

Secondly, data might have to be categorised as personal data because different NCCs have additional information and can, by linking different information and data, identify an individual. In this context the storage period also has to be considered. In most cases the shared information should lead to an interception of vessels or another legal or administrative measure. Consequently, at least the acting state will gather further information about the individuals and therefore be able to identify the persons and relate the previous information (such as the port of departure) to them.

Finally, the purpose and the result of EUROSUR, make it necessary to categorise parts of the exchanged data as personal data. If the purpose of the data processing is the identification of the surveilled individuals or the use of the information will impact the rights and interests of these individuals,[59] the whole application as such has to be considered as processing data relating to identifiable persons, even if some persons are not identifiable in practice.[60] When examining the creation of EUROSUR the European Commission stated as one of the objectives for the new system the reduction of irregular – 'illegal' according to the Commission – migration. Further explanatory remarks show that the purpose of EUROSUR is to provide the authorities responsible for border control in the Member States with more timely and reliable information, so they are able to detect, identify and intercept those attempting to enter the EU.[61] Therefore, the identification of irregular migrants is one of the objectives of EUROSUR and thus, one of the purposes of the data exchange. Moreover, the data exchange will impact the interests of specific persons, since EUROSUR shall improve

> *the ability to monitor, detect, identify, track and understand cross-border activities in order to find reasoned grounds for reaction measures on the basis of combining new information with existing knowledge.*[62]

Reaction measures will include interceptions, controls, arrests, etc. and consequently affect person's rights and interests.

In conclusion, while there is no hard evidence available that personal data is exchanged in the EUROSUR Network, since the relevant documents are not publicly available, the examples from the user interface, the data processed in the NCCs as well as the objectives of EUROSUR support the presumption that personal data is exchanged between the NCCs themselves as well as Frontex and the NCCs. Consequently, it will be assumed that the data exchange element of EUROSUR also interferes with the right to privacy and protection of personal data.

3.1.3 Seriousness of the Interference

Since both core elements of EUROSUR interfere with the right to privacy and data protection, it has to be established how serious the interference is. While there are several problematic points concerning EUROSUR, the most concerning one is the sheer amount of different data and data sources that are compiled in EUROSUR. The regulation only entails a non-exhaustive list of sources and therefore provides Frontex and the responsible national authorities with a margin of appreciation to include all data and data sources which they deem necessary for achieving the objectives of the regulation. Furthermore, Frontex is obliged to intensify their cooperation with international organisations and European Union bodies to make use of existing information and available capabilities and systems. While some of the examples stated in the regulation are obvious, such as EUROPOL or the Maritime Analysis and Operations Centre – Narcotics, others are not, such as the European Fisheries Control Agency. Furthermore, the European Space Agency (ESA) is now cooperating with Frontex and ESA's programme Copernicus[63], which was founded to provide information regarding the environment and climate change, is now providing Frontex with satellite imagery.[64] Similar cooperation is encouraged on a national level, and Member States shall increase their cooperation and data exchange with third countries and regional networks.[65]

Correlating to the amount of sources is the amount of affected persons. The satellite used in the Copernicus programme is able to capture an area as wide as 290 km[66] and the OPA Frontex is interested in has the capability to surveil an area for 12,5 hours without refuelling.[67] Furthermore, it has to be considered that in particular the southern European Coasts and the Mediterranean Sea, were most of the surveillance is taking place, is frequently used for leisure purposes during the summer months by many tourists.[68] Additionally, the regulation does not only oblige Frontex to monitor the sea itself but also third country ports and coasts. Since satellites do not enable a specific and targeted surveillance, but create a general image of an area it can be assumed that the common application of surveillance tools will constitute a general surveillance of the area around the European external borders.[69] Consequently, it will include the collection of excessive information concerning everyone present at or around the external borders.

A similar open approach is taken in the regulation regarding the recipients of information.[70] Besides Frontex and all participating states the information shall be shared with European Union bodies, offices and agencies, and international organisations[71] as well as with regional networks and, under certain circumstances, with neighbouring third countries.[72] On a national level the NCC shall distribute the information to all authorities with a responsibility for external border surveillance as well as with law enforcement, asylum, and immigration authorities.

Furthermore, EUROSUR entails the possibility to process special categories of data, which are normally stronger protected in European Data Protection Laws.[73] These categories include information regarding racial or ethnic origin, political opinions or religious or other beliefs, as well as personal data concerning health and sexual life or criminal convictions.[74] Surveilling ports or towns, or tracking vessels – including photographic surveillance – for an extended period of time might reveal information regarding person's habits to visit religious institutions or to pray and thereby disclose one's religious beliefs. Furthermore, the incident reports of the situational picture may reveal criminal convictions, and descriptions of the involved persons can entail their ethnic origin.

The next point of concern relates to transparency – or rather the lack of it – as well as the supervision of EUROSUR. Most of the documents revealing the exact scope of data exchange are not publicly available and therefore an exact scrutiny is not possible. Furthermore, since the system is running 24 hours a day, 7 days a week and includes inter alia the possibility of audio and video conferencing this unrecorded exchange of information complicates the general difficulty of supervising large-scale international, interconnected databases even more.[75] From the point of view of the data subject, transparency would be of upmost importance to ascertain which authority has which information about oneself. Nonetheless, this seems rather illusory in the context of EUROSUR. Once a NCC inserts information into its National Situational Picture it will be automatically shared with Frontex and the other NCCs, including all the national or international authorities they are further connected with. Only the transfer of information to third countries requires the consent of the NCC which provided the original information. Consequently, not even the NCCs know to which authorities in Europe the information is disclosed. Further concerns are raised by the planned as well as deployed surveillance tools, such as RPAS and satellites. While the use of these tools is openly communicated,

> *data subjects would hardly be aware of this kind of processing as it is difficult to notice RPAS, because of their small size and the altitude of operation. Furthermore, it is difficult, if not impossible, even for individuals noticing such devices, to know who is observing them, for what purposes and how to exercise their rights*.[76]

This combination of abstract knowledge regarding surveillance in a certain area but further uncertainty can, according to the ECJ, "*generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."*[77] A further problem of secret surveillance was pointed out by the ECtHR in the *Klass case*[78]:

> *The Court points out that where a State institutes secret surveillance the existence of which remains unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, Article 8 (art. 8) could to a large extent be reduced to a nullity. It is possible in such a situation for an individual to be treated in a manner contrary to Article 8 (art. 8), or even to be deprived of the right*

> *granted by that Article (art. 8), without his being aware of it and therefore without being able to obtain a remedy either at the national level or before the Convention institutions.*[79]

A further factor that elevates the intensity of the interference is the potential abuse of stored data.[80] Notwithstanding the data protection obligations entailed in the EUROSUR Regulation, the system itself and the large-scale collection of data increase the risk of misuse of personal information. As explained before, the user interface allows data exchange via text boxes and does not include any privacy enhancing or depersonalising safeguards. Furthermore, neither the system itself nor the EUROSUR Regulation hinder or permit that the description of an event is illustrated with attached images or videos. As asylum and immigration authorities shall also be provided with relevant information, these might run an asylum seeker's photo against all the uploaded EUROSUR pictures of arrivals by sea to ascertain where he/she first landed or authorities in charge of tracing unaccompanied minors' family members may wish to consult EUROSUR pictures to see if the child arrived accompanied by adults. While both examples are unintended by the regulation they are not only technical possible but also not prohibited by it.[81]

Last but not least, the general application of surveillance or the lack of reasoned grounds for surveillance aggravates the intensity of the interference. EUROSUR aims at finding reasoned grounds for reaction measures on the basis of combining new information with existing knowledge.[82] However, while the objective might be justified, the definition shows that there does not have to exist any initial suspicion or indication. Consequently, all persons who stay, roam or sail in a certain area will be put under a general suspicion until they are categorised as unsuspicious. This can also be seen in the regulation itself, since according to Art. 9 (3) (d) the event layer shall contain *information on unidentified and suspect vehicles, vessels and other crafts and persons at, along or in the proximity of the external border*. The ECJ categorised the Data Retention Directive[83] as a particular serious interference with the right to private life partly because it applied even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.[84]

In summary, it can be argued that EUROSUR constitutes a rather serious interference with the right to privacy, even though no personal data in the traditional sense of the term – meaning information about an already identified person – is processed.[85] It has to be reiterated that "*to establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way.*"[86] In particular the general application of surveillance without any reasoned grounds combined with the vast range of data sources and data recipients aggravate the interferences. However, this already grave interference is further intensified by the lack of transparency and the correlating exclusion of data subjects' rights.

3.2 Justification of EUROSUR

After establishing that EUROSUR interferes with fundamental rights it further has to be ascertained if the interference is justified. According to Art. 8 (2) ECHR an interference is justified if it is in accordance with law, if the restriction targets one of the listed legitimate aims, and if the interference is necessary in a democratic society. A set of similar requirements apply to interferences with rights of the EUFRCh.

> *Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*[87]

3.2.1 Accordance with law

To be in accordance with law, the interference has to not only be based on a national or European law,[88] which is accessible to the citizens, but the law also has to be formulated with sufficient precision, allowing citizens to foresee the consequences which a given action may entail.[89] While this so-called test of foreseeability does not require that the law stipulates every detail of surveillance, the legal foundation should not give the executive

authorities an excessively broad discretion. "*The law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."*[90]

> *The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law.*[91]

When applying these guidelines towards the EUROSUR Regulation the following conclusion can be drawn. Firstly, every inclusion of personal data in the European Situational Picture or the Common Pre-Frontier Intelligence Picture that is not concerning ship identification numbers is illegal, since there is no legal foundation.[92] However, there are sufficient safeguards in place for personal data concerning ship IDs. Secondly, personal data in the National Situational Picture is hardly safeguarded in the regulation, since the only provision concerning the protection of personal data is a general cross reference to European and national provisions on data protection. Consequently, there are no EUROSUR specific safeguards in place. This, however, appears as a surprise, since the Commission stated in 2008 that:

> *The processing of personal data within the context of EUROSUR must therefore be based on appropriate legislative measures, which define the nature of the processing and lay down appropriate safeguards.[93]*

Furthermore, the Commission was encouraged in this endeavour by the Article 29 Working Party, which states that even the exchange of personal data to a limited extent would require specific boundaries concerning the scope and categories of personal data, and its limited use and retention.[94] Moreover, the possibility that personal data is processed in the common application of surveillance tools is not mentioned once in the regulation. As a result, it has to be concluded that the limitations to the right of privacy based on the EUROSUR Regulation cannot be justified due to the vagueness of the provisions and the lack of safeguards. As it has been explained above, the data sources and recipients are specified in non-exhaustive lists, the information exchanged is only described vaguely, there are no specific safeguards or remedies, and all relevant decisions are made by the executive authorities in the Member States or Frontex without any direction provided by the regulation. Consequently, the EUROSUR Regulation is not formulated precise enough to qualify as justifying law. In this context it also has to be noted that the legal basis for EUROSUR was negotiated after or at least parallel to the creation of the system. After running pilot projects between 2008 and 2011 by year-end of 2012 Frontex signed a Memorandum of Understanding with 18 Member States and connected them to EUROSUR, one year prior to the adoption of the regulation.

3.2.2 The Essence of Fundamental Rights and Legitimate Aims

Furthermore, it is questionable if the regulation respects the essence of the right to privacy and data protection as required by Art. 52 (1) EUFRCh. European data protection organisations have declared that:

> *The monitoring of travellers has to be well founded and can only be allowed in exceptional cases and for justified and specific purposes. Any general surveillance poses unacceptable risks to the freedom of individuals.*[95]

> *From its analysis, the Working Party concludes that secret, massive and indiscriminate surveillance programs are incompatible with our fundamental laws and cannot be justified by the fight against terrorism or other important threats to national security.*[96]

Nonetheless, EUROSUR does not include a targeted surveillance of people entering Europe, but rather a surveillance of specific areas. Furthermore, the surveillance does not interfere with the core personal sphere but rather with individuals in public or in transit. "*Such an individual in transit may well expect a lesser degree of privacy, but not expect to be deprived in full of his rights and freedoms as also related to his own private sphere*

and image."[97] As EUROSUR does not deprive individuals fully of their privacy, it does respect the essence of their data protection right.

Furthermore, the purposes of EUROSUR of "*detecting, preventing and combating illegal immigration and cross-border crime and contributing to ensuring the protection and saving the lives of migrants*"[98] are legitimate aims (national security, public safety, prevention of crime, amongst others).

3.2.3 Necessary in a Democratic Society

Last but not least, the interference has to be necessary in a democratic society. According to the jurisdiction of the ECtHR this necessity test consists of two elements:[99]

- Does the interference correspond to a pressing social need?
- Is the interference proportionate to the legitimate aim? / Is the interference no greater than necessary to address the pressing social need?

Therefore, each of the purposes has to constitute a current pressing social need. While the European Union has a certain margin of appreciation in determining pressing social needs, there has to be at least factual evidence that an issue exists that needs to be addressed with a view to protecting public security. Furthermore, EUROSUR actually has to contribute to tackling the issue.

In general, it cannot be questioned that an effective management and control of the external borders of the European Union is necessary and a social need. Nonetheless, justification of interferences with fundamental rights requires that the tool in question corresponds to a specific issue which requires an urgent response. According to the EUROSUR Regulation and the correlating documents the main goal of EUROSUR is to combat irregular migration into the EU, while the prevention of loss of life at sea as well as fighting cross border crime are only added advantages.[100] However, already in 2008 – when the EUROSUR Regulation was firstly initiated – the European Data Protection Supervisor criticised the proposal for the lack of evidence of the necessity and the lack of evaluation of existing systems.[101] In the following years, the relevant authorities have neither responded to the existing criticism nor have they considered the changes in migration flows. Consequently, several arguments can be produced that question the necessity of EUROSUR.

Firstly it seems that the European Union has a disproportionate focus on irregular arrivals by land and sea.[102] Statistics show, that only a very small percentage of migrants enter Europe irregularly by sea or land, while the majority of migrants without the required documents overstay their visas.[103] Furthermore, it has to be considered, that a vast majority of the migrants arriving by sea are in the need of protection and apply for asylum or another form of protection.[104] In this context it also has to be stressed, that within the European Union irregular migration is still considered a security problem and linked to terrorism and cross border crime.[105] Similarly does the term 'illegal migration' – as used in the EUROSUR Regulation – suggest that irregular migration is a criminal offence in line with human trafficking. Nonetheless, the UNHCR[106] has emphasised repeatedly that irregular migration does not constitute a criminal offence and that the 1951 Geneva Convention[107] explicitly prohibits penalties relating to the illegal entry of refugees. Moreover, the terminology is not only regrettable,[108] but "*defining persons as illegal can also be regarded as denying their humanity*"[109] and challenging their fundamental rights as human beings. Consequently, the issue of irregular migration should not be approached with the same means as the smuggling of humans or contraband. Furthermore, there is no reliable data linking irregular migration to terrorism or proving that the majority of those entering irregularly are serious criminals[110] and the perception of 'migrant criminality' is wrong in most cases.[111]

Secondly, the statistics of the last decade have shown, that the number of migrants entering into Europe is declining – except a short incline resulting from the Arab spring and ongoing civil unrest and war.[112] Nonetheless, the proposal for the EUROSUR Regulation from 2008 has not been abandoned or changed. Furthermore, it is unlikely that migration will be stopped by reinforcing border control or other border management measures. So far statistics have proven that increased surveillance or control measures in one area of the border do not result in a cease of migration but in a shift of migration routes, and consequently longer and

more dangerous trips for migrants.[113] Furthermore, experiences have already been made with a large-scale high-tech surveillance network (SBI-net) at the border between Mexico and the US since 2006. As a result, the funding of the project was frozen in 2010 and the initiative consequently stopped and seriously altered since the project in its original form did neither meet its capacities nor provide the authorities with the necessary assistance.[114]

According to the Commission EUROSUR will also affect the fight against serious crime in Europe, since "*criminal networks involved in the smuggling of migrants are often using the same routes and methods for cross-border crime activities, such as trafficking in human beings, illicit drug trafficking, illicit arms trafficking, trafficking in radioactive and nuclear substances, and terrorism."*[115] While the linkage between migrants and terrorism has already been discussed above, the described 'use of the same routes' can also be questioned. Since 2003 testimonies of arriving migrants show that normally one of the migrants themselves operates the vessel.[116] Due to increased surveillance and interceptions and a heightened risk of being arrested on sea or upon arrival smugglers are hardly ever on board of the boats.[117] Moreover, it has to be stressed that so far the UN Smuggling Protocol, which is part of the Organised Crime Convention, has never been invoked as legal basis for interceptions during Frontex missions. Therefore, it seems not only questionable that these routes are also used for the trafficking of other goods but also that any arrests would be foreseeable. In the context of serious cross border crimes it further has to be mentioned that abetting or facilitating 'illegal' immigration, which carries a penalty of up to 15 years imprisonment in Italy, is also applied to fishermen or other sailors who render assistance to migrant boats.[118] The *Cap Anamur* case[119] and other cases proved that even though the law contains an exemption if assistance is given to those in need, the exemption is applied restrictively and that it is not clear if it is also valid in cases where the assistance is given outside of the Italian territorial waters.[120]

Finally, it is questionable how much EUROSUR can actually contribute towards *protection and saving the lives of migrants*.[121] While the high number of migrants' deaths on the way to the Europe is caused in various ways – including suffocation in trucks, car accidents, frostbite, police violence, hunger strikes, landmines, or suicide in detention[122] – the majority loses their lives at sea. Even though the Mediterranean Sea is already one of the closest surveilled maritime spaces in the world, it is estimated that since the mid-1990s at least 20.000 migrants have died there.[123] Consequently, organisations such as the International Federation for Human Rights consider not the lack of information responsible for the death toll at European borders but rather the lack of legal possibilities to reach Europe, the shifting towards more hazardous routes, the reluctance of patrol and fishing vessels to render assistance, the conflicts over search and rescue responsibilities, and the unwillingness of the EU to tackle the root causes of migration.[124] Yet, besides a general statement to contribute towards search and rescue of migrants in distress, the EUROSUR Regulation does not entail any provisions on how exactly this contribution will look like. Currently there are no official procedures detailing how to proceed after a distress-call nor is there an obligation to include national authorities responsible for search and rescue into EUROSUR or the NCC.[125] Additionally, it has to be stressed that surveillance measures on their own are not capable of saving lives. This can be illustrated by a report from a Major of the Maltese Armed Forces in front of the UK House of Lords: After a distress call of a vessel a Maltese aircraft was send to the scene but after some time "*the aircraft was withdrawn for refuelling and sent again to the position. On arriving it did not find a boat either in the position where it had been initially sighted nor within a substantial radius around it*."[126] In conclusion, the UN Special Rapporteur on the human rights of migrants "*fears that EUROSUR is destined to become just another tool that will be at the disposal of member States in order to secure borders and prevent arrivals, rather than a genuine life-saving tool."*[127]

In sum, the introduction of the EUROSUR does not seem necessary in a democratic society. While the aims of the regulation are comprehensible, the accompanying documents do not show how EUROSUR will be able to contribute towards achieving these goals. Furthermore, there is no hard evidence that an additional surveillance tool is necessary at the European borders. Neither the proposal of the EUROSUR Regulation nor the following documents have evaluated the already increased surveillance and interception operations of Frontex, the intensified cooperation of Member States in regional networks and with third countries, or the decrease of migrants. However, this would have been necessary to prove that additional measures were necessary in 2008 and still are.

Finally, each interference has to be proportionate, meaning that an interference should not be greater than necessary. From the regulation itself as well as from the accompanying documents and press releases it can be concluded that the EU deems the collection, storage and exchange of personal data generally as not necessary for achieving the goals of EUROSUR. Consequently, the current version of EUROSUR is not proportionate since it gives the actors the possibility and the legal grounds to process personal data. Several properties of the current user interface as well as the common application of surveillance tools could have been implemented less intrusive by following a privacy-by-design approach. Furthermore, this would have limited the possibilities of misuse. The current regulation obliges Member States and Frontex to process data in accordance with the European and national provisions on data protection. However, it does not foresee any specific legal, organisational or technical safeguards. Nonetheless, in particular the latter one would have been desirable, since it can already be observed in the context of border control management "*that where strong human rights standards are incorporated into European Union policy and legislation, there is often a wide discrepancy between the texts and member-State implementation*."[128] In conclusion, the interference by the current EUROSUR system is greater than necessary since a more privacy protecting version seems possible.

4 Conclusion

A more privacy protecting system and regulation would have to observe the following recommendations. Firstly, the regulation should include provisions outlining the exceptional reasons and circumstances in which the processing of personal data is permitted as well as which data will be collected and shared. Furthermore, it should exhaustively list all data sources. This list should result from a thorough evaluation of each source under necessity considerations which should be included into the accompanying documents of a new regulation. A similar procedure is advisable for the recipients of data. Moreover, after the actual exchange of data, the recipients – European and national authorities – should be recorded in the system itself. Additionally, the inclusion of obligatory deletion deadlines as well as organisational and technical measures to protect the personal data is necessary. Concerning the system itself, the EU should abstain from using free text boxes to prevent misuse. Furthermore, the possibility to add historical or photographic information to an incident should be abandoned, since it increases the likelihood of persons being identified via the system. Moreover, when applying common surveillance tools, the possibility to identify individuals should be precluded. Therefore, no sensors or cameras should be used that provide a high resolution or zoom capabilities enabling the identification of persons from the recorded images. These improvements could contribute towards a regulation that is more compliant with the right to privacy not only in consideration of the proportionality requirement but also under the aspect of the precision of the legal foundation. Nonetheless, even these improvements will not resolve the issues regarding the necessity of a new surveillance system at the European borders. Furthermore, this paper analysed EUROSUR only from a privacy protection point of view and all the existing issues concerning other fundamental rights of migrants have been left aside.

While there are currently no drones securing European borders, Baroness Ludford was, nevertheless, right, when she warned about the route the European Union is taking in the context of border management. The EUROSUR Regulation is just one of the examples that prove that due to security concerns – justified or not – the Member States are willing to neglect fundamental rights when balancing these competing interests. Furthermore, it shows that the tragedies of irregular migrants at sea are often used as an excuse for interfering with fundamental rights of refugees, asylum seekers, migrants as well as 'normal' travellers. While the deaths at sea of countless migrants are disgraceful for Europe it is very questionable that EUROSUR will improve this situation. Therefore, the criticism of the International Federation for Human Rights seems justified in the context of privacy protection, when they were stating:

> *The deaths in Lampedusa, like those from yesterday and from tomorrow, are the victims of a Europe that is locked to the point of obliviousness into a securitarian logic, which has renounced the values that it claims to defend.*[129]

1 Lucht, H.: *The Watery Tomb Europe Tolerates*, The New York Times, 7th October 2013; http://www.nytimes.com/2013/10/08/opinion/the-graveyard-at-europes-doorstep.html .

2 European Convention on Human Rights, hereinafter: ECHR.

3 Charter of Fundamental Rights of the European Union (2000/C 364/01), hereinafter: EUFRCh.

4 Goldirova, R.: *EU unveils plans for biometric border controls*; EUobserver, 13th February 2008; http://euobserver.com/justice/25650.

5 Pro Asyl: *EU-Asylpolitik nach Lampedus: Abschottung geht weiter*, 09.10.2013, http://www.proasyl.de/de/news/detail/news/eu_asylpolitik_nach_lampedusa_abschottung_geht_weiter-1/ .

6 Jesuit Refugee Service Europe: *Proposals for amendments to EUROSUR Regulation*

7 Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur), hereinafter: EUROSUR Regulation.

8 European Convention on Human Rights, hereinafter: ECHR.

9 Charter of Fundamental Rights of the European Union (2000/C 364/01), hereinafter: EUFRCh.

10 Art. 1 EUROSUR Regulation.

11 Art. 3 (b) EUROSUR Regulation.

12 European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union; established by Regulation (EC) No 2007/2004; hereinafter: Frontex.
The name of EU's external border agency derives from the French term *frontiers extérieures* (external borders).
Its main responsibilities are the following:
- Planning, coordination and implementation of joint border control operations;
- Training of national border guards;
- Risk analysis, research and intelligence gathering;
- Provision of rapid response capabilities;
- Assisting in deportations;
- Information exchange.

For more information see: http://frontex.europa.eu/ .

13 The list of sources entailed in Art. 9 (2) EUROSUR Regulation includes ten different sources for relevant information; nevertheless by further including 'others' the list is not exclusive and gives the Member States an extensive margin of appreciation to collect information from every source possible.

14 Art. 9 (3)(d) EUROSUR Regulation.

15 E.g. EUROSUR Handbook.

16 An overview can be found in the European Commission Staff Working Paper SEC(2011) 1538 final, Annex 1.

17 European Union: *Infographic European Border Surveillance System (EUROSUR)*, http://ec.europa.eu/dgs/home-affairs/e-library/multimedia/infographics/index_en.htm#080126248ad359ff/c_ .

18 Art. 12 EUROSUR Regulation.

19 ECtHR, App. 6825/74, *X v Iceland*, Decision of 18 May 1976, (1976) 5 DR 86; ECtHR, App. 23841/95, *Rotaru v Romania*, 4 May 2000 [GC], ECHR 2000-V, § 46; ECtHR, App. 27798/95, *Amann v Switzerland*, 16 February 2000 [GC], ECHR 2000-II, § 65.

20 European Court of Justice, hereinafter: ECJ.

21 European Court of Human Rights, hereinafter: ECtHR.

22 Article 29 Data Protection Working Party: *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, adopted on 27 February 2014, p. 4.

23 ECtHR, App. 44647/98, *Peck v United Kingdom*, 28 January 2003, ECHR 2003-I.

24 Ibid. § 59.

25 Ibid. § 59.

26 ECtHR, App. 23841/95, *Rotaru v Romania*, 4 May 2000 [GC], ECHR 2000-V.

27 ECtHR, App. 27798/95, *Amann v Switzerland*, 16 February 2000 [GC], ECHR 2000-II.

28 ECtHR, App. 23841/95, *Rotaru v Romania*, 4 May 2000 [GC], ECHR 2000-V, § 43 - 44; ECtHR, App. 27798/95, *Amann v Switzerland*, 16 February 2000 [GC], ECHR 2000-II, § 65 - 67.

29 ECtHR, App. 23841/95, *Rotaru v Romania*, 4 May 2000 [GC], ECHR 2000-V, § 43.

30 ECtHR, App. 9248/81, *Leander v Sweden*, 26 March 1987, Series A No 116.

31 Art. 2 (a) 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; Art. 2 (a) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Art. 2 (a) Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

32 Article 29 Data Protection Working Party: *Working Document on the Processing of Personal Data by means of Video Surveillance*, adopted on 25 November 2002, p. 5.

33 Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, adopted on 20 June 2007, p. 8.

34 Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, adopted on 20 June 2007, p. 10.

35 Ibid. p. 11.

36 Ibid. p. 11.

37 European Union Agency for Fundamental Rights: *Handbook on European Data Protection Law*, Luxembourg,

Publications Office of the European Union, 2014, p. 39.

38 Article 29 Data Protection Working Party: *Opinion 4/2007 on the concept of personal data*, adopted on 20 June 2007, p. 13.

39 Ibid. p. 13, 21.

40 Ibid. p. 16.

41 Article 29 Data Protection Working Party: *Letter to the Commissioner for Home Affairs Ms. Cecilia Malmström regarding the Proposal for a Regulation establishing the European Border Surveillance System,* p. 2.

42 European Commission: *Communication from the Commission to the European Parliament and the Council on the work of the Task Force Mediterranean*, COM (2013) 869 final, Brussels, 4.12.2013, p. 17.

43 Article 29 Data Protection Working Party, *Letter to the Commissioner for Home Affairs Ms. Cecilia Malmström regarding the Proposal for a Regulation establishing the European Border Surveillance System,* p. 2.

44 Art. 12 (3) EUROSUR Regulation.

45 European Union Agency for Fundamental Rights: *Fundamental rights at Europe's southern sea borders*, Luxembourg, Publications Office of the European Union, 2013, p. 60.

46 Zöller, M. A., Ihwas, S. R.: *Rechtliche Rahmenbedingungen des polizeilichen Flugdrohneneinsatzes*, Neue Zeitschrift für Verwaltungsrecht, 2014, p. 408 – 414, 410.

47 Ludwig, A.: *Frontex und Eurosur – Umweltsatelliten der Esa helfen bei Jagd auf Flüchtlinge*, Zeit Online, 20th December 2013; http://www.zeit.de/digital/datenschutz/2013-12/frontex-eurosur-satelliten-fluechtlinge .

48 Nielsen, N.: *EU looks to 'hybrid drones' for legal shortcut on migration*, EUobserver, 14th October 2013; http://euobserver.com/priv-immigration/121735.

49 Article 29 Data Protection Working Party: *Letter to the European Commission regarding Remotely Piloted Aircraft Systems (RPAS) – Response to the Questionnaire*, p. 1.

50 Hayes, B., Vermeulen, M.: *Borderline – EU Border Surveillance Initiatives – An Assessment of the Costs and Its Impact on Fundamental Rights*, Berlin, Heinrich Böll Stiftung, 2012, p. 38.

51 European Commission: *Proposal for a Regulation of the European Parliament and of the Council Establishing the European Border Surveillance System (EUROSUR)*, COM (2011) 873 final, Brussels, 12.12.2011, p. 3.

52 European Commission: *EUROSUR: new tools to save migrants' lives at sea and fight cross-border crime*, Memo/13/578, Brussels, 19th June 2013.

53 Art. 13 EUROSUR Regulation.

54 European Union Agency for Fundamental Rights: *Fundamental rights at Europe's southern sea borders*, Luxembourg, Publications Office of the European Union, 2013, p. 62; Recital 13 EUROSUR Regulation.

55 European Commission: *Commission Staff Working Paper - Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR)*, SEC(2011) 1538 final, Brussels, 12.12.2011, p. 31, 32.

56 Article 29 Data Protection Working Party: *Opinion 05/2014 on Anonymisation Techniques*, adopted on 10 April 2014, p. 9.

57 European Union Agency for Fundamental Rights: *Fundamental rights at Europe's southern sea borders*, Luxembourg, Publications Office of the European Union, 2013, p. 6o.

58 Ibid. p. 62.

59 Article 29 Data Protection Working Party: *Opinion 4/2007 on the concept of personal data*, adopted on 20 June 2007, p. 11.

60 Ibid. p. 16.

61 European Commission: *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, 13.02.2008, p. 3.

62 Art. 3 (b) EUROSUR Regulation.

63 http://www.esa.int/Our_Activities/Observing_the_Earth/Copernicus .

64 Ludwig, A.: *Frontex und Eurosur – Umweltsatelliten der Esa helfen bei Jagd auf Flüchtlinge*, Zeit Online, 20th December 2013; http://www.zeit.de/digital/datenschutz/2013-12/frontex-eurosur-satelliten-fluechtlinge.

65 European Commission: *Communication from the Commission to the European Parliament and the Council on the work of the Task Force Mediterranean*, COM (2013) 869 final, Brussels, 4.12.2013, p. 5 – 11.

66 Ludwig, A.: *Frontex und Eurosur – Umweltsatelliten der Esa helfen bei Jagd auf Flüchtlinge*, Zeit Online, 20th December 2013; http://www.zeit.de/digital/datenschutz/2013-12/frontex-eurosur-satelliten-fluechtlinge.

67 Nielsen, N.: *EU looks to 'hybrid drones' for legal shortcut on migration*, EUobserver, 14th October 2013; http://euobserver.com/priv-immigration/121735.

68 European Union Agency for Fundamental Rights: *Fundamental rights at Europe's southern sea borders*, Luxembourg, Publications Office of the European Union, 2013, p. 6o.

69 International Working Group on Data Protection in Telecommunications: *Arbeitspapier zum Datenschutz bei Überwachung aus der Luft*, Berlin , 54th Session, 2.-3. September 2013, p. 6.

70 European Data Protection Supervisor: *Preliminary Comments of the European Data Protection Supervisor on: COM(2008) 69 final; COM(2008) 68 final; COM(2008) 67 final*, Brussels, 3rd March 2008, p. 7.

71 Art. 18 EUROSUR Regulation.

72 Art. 20 EUROSUR Regulation.

73 For example: Art. 8 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, Art. 6 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

74 Only the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data includes information regarding criminal convictions.
75 European Data Protection Supervisor: *Preliminary Comments of the European Data Protection Supervisor on: COM(2008) 69 final; COM(2008) 68 final; COM(2008) 67 final*, Brussels, 3rd March 2008, p. 7.
76 Article 29 Data Protection Working Party, *Letter to the European Commission regarding Remotely Piloted Aircraft Systems (RPAS) – Response to the Questionnaire*, p. 1, 2.
77 ECJ, *Digital Rights Irleand Ltd.*, C-293/12 and C-594/12, Judgement of 8th April 2014, § 37.
78 ECtHR, App. 5029/71, *Klass and others v Germany*, 6 September 1978, Series A No. 28.
79 Ibid. § 36.
80 Advocate General Cruz Villalon (ECJ), *Digital Rights Irleand Ltd.*, C-293/12 and C-594/12, Opinion, 12th December 2013, § 75.
81 European Union Agency for Fundamental Rights: *Fundamental rights at Europe's southern sea borders*, Luxembourg, Publications Office of the European Union, 2013, p. 62.
82 Art. 1, 3 (b) EUROSUR Regulation.
83 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
84 ECJ, *Digital Rights Ireland Ltd.*, C-293/12 and C-594/12, Judgement of 8th April 2014, § 58.
85 Advocate General Cruz Villalon (ECJ), *Digital Rights Irleand Ltd.*, C-293/12 and C-594/12, Opinion, 12th December 2013, § 74.
86 ECJ, *Digital Rights Ireland Ltd.*, C-293/12 and C-594/12, Judgement of 8th April 2014, § 33.
87 Ibid. § 38.
88 ECtHR, App. 45036/98, *'Bosphorus Airways' v Ireland*, 30 June 2005, 2005-VI.
89 ECtHR, App. 6538/74, *Sunday Times v United Kingdom*, 26 April 1979, Series A No. 30, § 49.
90 White, R. C.A., Ovey, C.: *The European Convention on Human Rights*, New York, Oxford University Press, 2010, 5th Edition, p. 367.
91 ECtHR, App. 5029/71, *Klass and others v Germany*, 6 September 1978, Series A No. 28, § 50.
92 Art 13 (2) EUROSUR Regulation.
93 European Commission: *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, 13.02.2008, p. 11.
94 Article 29 Data Protection Working Party: *Letter to the Commissioner for Home Affairs Ms. Cecilia Malmström regarding the Proposal for a Regulation establishing the European Border Surveillance System*, p. 1, 2.
95 Conference of the European Data Protection Authorities: *Border Management Declaration*, Rome, April 2008.
96 Article 29 Data Protection Working Party: *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, adopted on 10 April 2014, p. 2.
97 Article 29 Data Protection Working Party: *Working Document on the Processing of Personal Data by means of Video Surveillance*, adopted on 25 November 2002, p. 5.
98 Art. 1 EUROSUR Regulation.
99 See for example: ECtHR, Apps 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, and 7136/75, *Silver v United Kingdom*, 25 March 1983, Series A No. 61, § 97.
100 European Commission: *Commission Staff Working Paper - Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR)*, SEC(2011) 1538 final, Brussels, 12.12.2011, p. 8, 9.
101 European Data Protection Supervisor: *Preliminary Comments of the European Data Protection Supervisor on: COM(2008) 69 final; COM(2008) 68 final; COM(2008) 67 final*, Brussels, 3rd March 2008, p. 3, 4.
102 UN Human Rights Council: *Report of the Special Rapporteur on the human rights of migrants, Regional study: management of the external borders of the European Union and its impact on the human rights of migrants*, 24 April 2013, A/HRC/23/46, p. 6.
103 Ibid; European Union Agency for Fundamental Rights: *Fundamental rights at Europe's southern sea borders*, Luxembourg, Publications Office of the European Union, 2013, p. 19 – 23.
104 According to statistics (from 2009) roughly 70% of the migrants that arrived in Malta by sea applyed for asylum; (UNHCR: *Irregular Migration by Sea: Frequently Asked Questions*, http://www.unhcr.org/4a1e48f66.html).
105 See for example: European Commission, *Commission Staff Working Paper - Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR)*, SEC(2011) 1538 final, Brussels, 12.12.2011, p. 8, 9.
106 United Nations High Commissioner for Refugees, hereinafter: UNHCR.
107 Art. 31 1951 Convention Relating to the Status of Refugees, hereinafter: 1951 Geneva Convention.
108 UN Human Rights Council: *Report of the Special Rapporteur on the human rights of migrants, Regional study: management of the external borders of the European Union and its impact on the human rights of migrants*, 24 April 2013, A/HRC/23/46, p. 10.
109 Koser K.: *Irregular migration, state security and human security*, Global Commission on International Migration, September 2005, p. 5.
110 European Data Protection Supervisor: *Preliminary Comments of the European Data Protection Supervisor on: COM(2008) 69 final; COM(2008) 68 final; COM(2008) 67 final*, Brussels, 3rd March 2008, p. 3.
111 Pugh, M.: *Mediterranean Boat People: A Case for Cooperation?*, Mediterranean Politics, 2001, 6, pp. 1–20, 2, 3.

112 European Union Agency for Fundamental Rights: *Fundamental rights at Europe's southern sea borders*, Luxembourg, Publications Office of the European Union, 2013, p. 19 – 23; Grant, H., Provost, C., Allen, P.: *Fortress Europe: have border controls worked? An interactive guide*, The Guardian, 13th January 2014, http:// www.theguardian.com/global-development/interactive/2014/jan/13/europes-border-control-interactive-guide .

113 Council of Europe – Parliamentary assembly: *Migration and asylum: mounting tensions in the Eastern Mediterranean*, 23 January 2013, Doc. 13106, p. 10, 15; Lutterbeck, D.: *Policing Migration in the Mediterranean*, Mediterranean Politics, 2006, 11 (1), pp. 59 – 82,74 – 77; Parliamentary Assembly of the Council of Europe: *Europe's "boat-people": mixed migration flows by sea into southern Europe – Report of the Committee on Migration, Refugees and Population*, Doc. 11688, 11 July 2008, para. 17.

114 Hayes, B., Vermeulen, M.: *Borderline – EU Border Surveillance Initiatives – An Assessment of the Costs and Its Impact on Fundamental Rights*, Berlin, Heinrich Böll Stiftung, 2012, p. 67.

115 European Commission: *Commission Staff Working Paper - Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR)*, SEC(2011) 1538 final, Brussels, 12.12.2011, p. 9.

116 European Union Agency for Fundamental Rights, *Fundamental rights at Europe's southern sea borders*, Luxembourg, Publications Office of the European Union, 2013, p. 25 – 27.

117 Hamood S.: *EU-Libya cooperation on migration: a raw deal for refugees and migrants?*, Journal of Refugee Studies, 2008, 21 (1), pp. 19 – 42, 29 – 31.

118 Parliamentary Assembly of the Council of Europe, *Europe's "boat-people": mixed migration flows by sea into southern Europe – Report of the Committee on Migration*, Refugees and Population, Doc. 11688, 11 July 2008, para. 36; ITF seafarers: *Damned if they do …*, http://www.itfseafarers.org/damned.cfm.

119 Information on the Cap Anamur case can be found at: Statewatch, *Italy: Criminalising Solidarity – Cap Anamur trial underway*, http://www.statewatch.org/news/2007/apr/03italy-cape-anamur.htm.

120 Ryan B., Mitsilegas, V.: *Extraterritorial immigration control: legal challenges* , Koninklijke Brill NV, Leiden, The Netherlands, 2010, p. 301

121 Art. 1 EUROSUR Regulation.

122 UN Human Rights Council: *Report of the Special Rapporteur on the human rights of migrants, Regional study: management of the external borders of the European Union and its impact on the human rights of migrants*, 24 April 2013, A/HRC/23/46, p. 6.

123 International Federation for Human Rights: *Lampedusa: Murderous Europe*, 10 October 2013.

124 Ibid.

125 European Union Agency for Fundamental Rights: *Fundamental rights at Europe's southern sea borders*, Luxembourg, Publications Office of the European Union, 2013, p. 62.

126 House of Lords European Union Committee, *9th Report of Session 2007 – 08, Frontex: The EU external borders agency*, Report with Evidence, London, United Kingdom, 5 March 2008, p. 19 (Box 1 – The disappearance of 53 Eritrean nationals)

127 UN Human Rights Council: *Report of the Special Rapporteur on the human rights of migrants, Regional study: management of the external borders of the European Union and its impact on the human rights of migrants*, 24 April 2013, A/HRC/23/46, p. 10, 11.

128 Ibid. p. 11.

129 International Federation for Human Rights: *Lampedusa: Murderous Europe*, 10 October 2013.