An Ethical Framework for Maritime Surveillance Technology Projects

Sari Sarlio-Siintola[a*], Tuomas Tammilehto[a], Saara Siintola[a,]
[a]Laurea University of Applied Sciences, Ratatie 22, 02200 Vantaa, Finland

ABSTRACT

The ethics of Maritime Surveillance is a topic of increasing importance in both academia and other forums. This development owes partially to new legal obligations, such as those set out in EUs new data protection legislation. Also the funders of innovation programs are increasingly expecting projects to pay attention to and address various ethical issues. The ethical challenges involved in the development and piloting of technology-based maritime surveillance solutions are multifaceted from both the research and development perspective, and from the viewpoint of the final solution to be created. The purpose of this paper is to present a framework for a) the identification of ethical, legal and societal aspects in technology innovation projects, and b) the operationalisation of these aspects as concrete requirements. Furthermore, in order to concretise the proposed framework, we discuss the outcomes of ethical analyses of two Horizon2020 maritime surveillance projects, MARISA and RANGER.

Keywords: Maritime Surveillance Technology, Ethical, Legal and Societal Aspects (ELSA), Responsible Research and Innovation (RRI)

1. INTRODUCTION

The ethics of Maritime Surveillance has been a topic for vivid discussions in both academia and various other forums, reports and statements. Especially concerns related to the tension between privacy and security on the other, has been a central focus in the debate.[1]Two centrepieces of EU law in the area of data protection, the General Data Protection Regulation ('GDPR'), and the Data Protection Law Enforcement Directive ('LED'), compel the carrying out of a specific Data Protection Impact assessment (PIA) prior to any processing of personal data that is likely to result in a high risk to the rights and freedoms of natural persons – including development work in maritime surveillance projects.
In addition to privacy-related concerns, the implications of new surveillance technologies for asylum seekers and refugees have been deliberated by several scholars.[2] [3] Due to the fact that both EU law and various international conventions regarding e.g. human rights, the rights of refugees, and Search and Rescue activities impose obligations on states to help and protect those in need, the increased situational awareness enabled by the new technologies will also lead to an increased responsibility to act.

The paper is organised as follows. In section two, we give a general introduction our approach to ethics work that covers both research and development processes, and the solution to be created during those processes. In section three, we present a methodology for identifying ethical, legal and societal aspects of technology projects aiming to produce innovations for the market. Finally, in section four, we discuss the operationalisation of the identified aspects as ethical requirements and guidelines for both technology and organisational arrangements.

[*]sari.sarlio@laurea.fi; phone +358 (0)40 513 9118; www.laurea.fi

2. ETHICAL DIMENSIONS OF TECHNOLOGY-BASED PROJECTS

Technology research and development projects are multidimensional from the point of view of ethics, legislation and societal impacts. In addition to traditional research integrity, it is essential to ensure also the comprehensive ethical and social sustainability of the solution being developed. Ultimately, sufficient ethical sustainability is a prerequisite for the social and political approval and market potential of any solution. Both research integrity, validation of the ethical features of the solution, and the use of beta versions in real time settings need to be addressed, also already during trials or other such tests (see Figure 1).

The ethical guidelines of Horizon2020 focus heavily on traditional research integrity-related issues and as such offer limited guidance in terms of the ethical and societal sustainability of real time setting piloting and trials, or the final product/solution itself. This can pose challenges for developers, for instance in projects that develop and pilot together with end users information systems (solutions) processing personal data; the implications of data protection related requirements can namely look very different for different aspects of the project.

From the research integrity perspective, the rights of end-users (and other natural persons) taking part in the projects must of course be secured. This may influence e.g. the collection of personal data or the dissemination of photos in which individuals can be identified. In addition to this, the solution itself must comply with numerous requirements set out in the GDPR and/or the LED, such as embodying the principles of Data Protection by Design and by Default. In other words, data protection must be integrated into the architecture by utilising privacy enhancing technologies or similar. Lastly, data protection compliance is required already during development and trials/pilots – the phase during which privacy and data protection features themselves are also being validated. In some cases the problem can be solved for instance by using fake data, but meaningful piloting often requires a real data. The take-home message is that ensuring data protection compliance is essential regardless of whether data protection issues are a central focus or purpose of the project.[1]

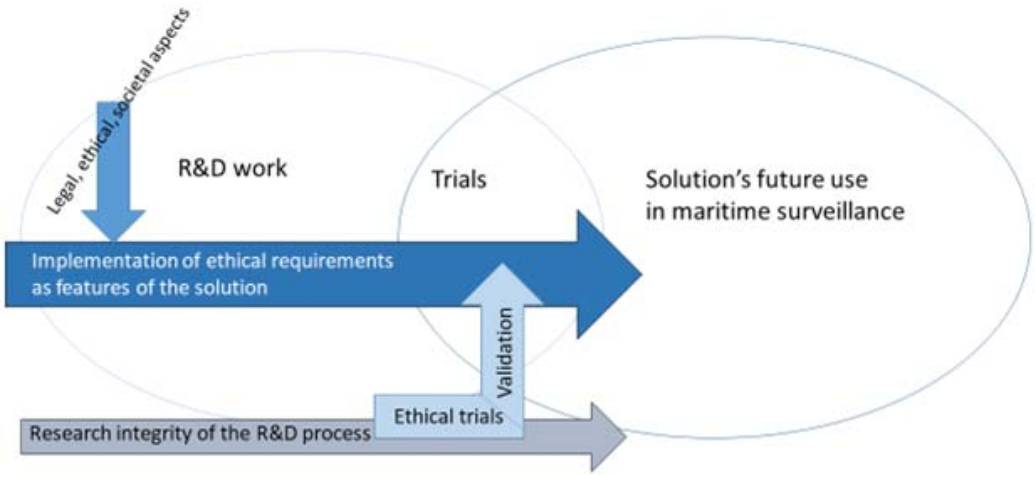

Figure 1 Ethical Dimensions in Technology-Based Projects

[1] An important thing to understand is that all data relating to an identified or identifiable person, directly or indirectly, constitutes personal data under the GDPR and the LED, and all processing of such data needs an explicit legal basis, such as a legal obligation or consent (Article 6). This means that for instance AIS data constitutes personal data, the processing of which falls under the scope of data protection legislation. As the installing and use of AIS could be interpreted as an expression of consent for the typical processing of such data this is normally not a problem.

In identifying the ethical challenges and opportunities that relate to the solution being created itself, a distinction should be made between the layers of technology, user processes, and business/governance models. This is essential, as the implications of ethical, legal and societal requirements often look different for different layers. Ethical requirements which can be implemented as technical features of the solution can be handled in the technical planning, implementation, and validation in a way that is analogous to end-user requirements. On the user process level, the implementation of ethical requirements concern for instance user manuals or administrative arrangements such as the training of users. On the business/governance models level, the relevant considerations could concern for example the division of responsibilities between different actors or various kinds of preparations and feasibility considerations to be done before implementing the solution into a specific environment.

Important is also to remember that the features of the developed solutions may vary according to the environment in which they will be implemented, which may have implications on ethical requirements on all layers of the solution. Both MARISA and RANGER, for instance, can be implemented as either stand-alone solutions or as part of the Common Information Sharing Environment (CISE). See Figure 2.

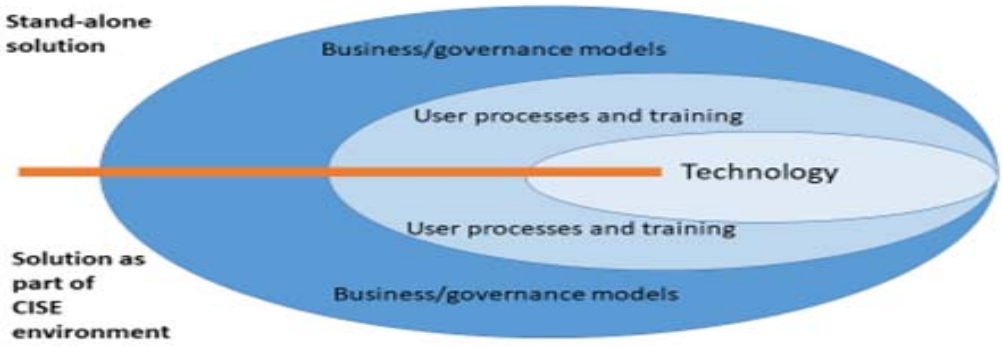

Figure 2: Ethical Layers of Technology-Based Solutions

3. THE METHOD OF ETHICAL ANALYSIS

Leeze et al. argue that ethics in security research must be seen as a way of putting critiques to work, not as a mere legitimising function of 'ethics approval'.[4] The same argument is widely discussed in the context of ELSA and RRI research. The approach we have developed during the MARISA and RANGER projects aims to provide a model/method/framework for doing just that. The purpose was to maximise the benefits of both projects while preventing or minimising any ethical risks.

In both MARISA and RANGER, we divided the analysis work into the following components: 1) a critical ethical analysis of the technology and its use in the relevant context (border control, customs, search and rescue, environment and general law enforcement), 2) a legal framework for the project (including development, the solution itself, and its future use), and 3) a Social Impact Assessment (SIA) and a Data Protection and Privacy Impact Assessment (PIA). The results of this work where then encapsulated into a set of concrete ethical requirements for the project, as well as a Code of Conduct containing ethical principles to be embedded both in training material and Business Model documentation.

We conducted the ethical analyses and the legal frameworks as desk-top studies where, among other things, we have analysed the content of various regulations, guidelines and policy papers. The SIA of each project was has carried out by having various stakeholders and experts do brainstorming work, the results of which were integrated in the project planning and risk management to mitigate potential problems and to promote positive impacts across the lifecycle of developments. The practice is participatory and it increases understanding of change and capacities to respond to change.[5] Central to the SIA approach is that ethical issues (concerning both positive and negative societal impacts) are taken into account already in the design-phase of innovation. Ethics are thus understood not only as legal and moral

constraints for innovation, but also as active catalyst of innovation from which value can be derived. The PIA work in MARISA and RANGER was organised in collaboration with project partners, utilising a PIA tool provided by CNIL (Commission Nationale de l'Informatique et des Libertés).

Key ethical challenges identified in the MARISA and RANGER projects are disclosed below, in Table 1.

Table 1: Main Ethical Challenges in the MARISA and RANGER Projects

Main Ethical Challenges in the MARISA and RANGER projects	
Challenges	Layers of the solution
Tensions between different rights and values, such as freedom and security, which are likely to become more pronounced as a result of the new security technologies.	- Business & governance models - User processes
Ethical and legal issues relating to privacy and data protection in both current and future configurations of RANGER and MARISA, including both technical and organizational arrangements	- Business & governance models - User processes - Technology
RANGER's impact on wildlife and humans in the region where the radars are installed. Regardless of whether the risks are real or only fears, it is ethically and societally important to address the issue.	- Business & governance models - Technology
Ethical and legal issues relating to OSINT, Big Data and AI in MARISA. These include the need for human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness (including awareness of and strategies to control subconscious biases), environmental and societal well-being, and accountability.	- Business & governance models - User processes - Technology

In the next step, the ethical, legal, and societal framework built as a result of the analysis work was refined into smaller, more detailed ethical requirements that were then categorised into the classes 'ethical awareness', 'ethical analysis' or '(any) activity'. At this stage the requirements should be specific and concrete enough to be associated with the relevant phase or layer of the project: pilots and trials, technology, user processes, business and governance model, or generally on the solution.

Finally, a specific Code of Conduct was formulated for each solution, based on the results of the analyses. The codes are designed for end-users, decision makers, and developers of the solution; the idea is that they shall be embedded both in training material and Business Model documentation..

4. THE RESULTS OF THE ANALYSIS AND THEIR IMPLMENTATION

The value bases of the ethical requirements and the Code of Conduct (for MARISA and RANGER) are derived from both fundamental human rights values and norms established in international and EU law, and various ethical issues raised by the end-users and other stakeholders.

The Code of Conduct establishes principles that should be taken into consideration when deploying, using and developing a solution, and concern the totality of ethical and societal considerations: the technology itself, how the technology will be used, as well as the whole business model/procurement as part of the European Maritime Surveillance ecosystem. A Code of Conduct should be subject to reviews and updates; when implementing a solution in a specific user community contexts, the principles are to be further specified and integrated into other existing codes of conduct. In the table 2, we list the main sections of the current versions of MARISA Code of Conduct and RANGER Code of Conduct.

Table 2: Contents of the RANGER and MARISA Code of Conducts

Code of Conduct (titles)
1 The Justification of MARISA/RANGER is Based on Ethical Grounds
2 The Humanitarian Imperative and the Rights of the People at Sea
3 Transparency, Liability and Human Decision Making
4 Privacy and Data Protection
5 Value for End-users Involvement
6 Moral Division of Labour in Maritime Surveillance and SAR
7 Robustness, Accountability and Learning

The ethical requirements defined must be taken into account in the technology development and organizational arrangements related to user process descriptions and training, as well as in governance- and business modelling. In the Table 3, here below, there are presented some ethical requirements of the MARISA project.

Table 3: Examples of MARISA's ethical requirements

(MARISA-G21) Recognize third countries in the sea as both end-users of MARISA, and as partners in solving shared problems with the help of new technology.	*Desirable/ Essential Activity* *MNGMT UC, AM,BM WP1, WP2*	*The MARISA Advisory Board include a representative from a third country. The point will be addressed during the MARISA workshops and the Advisory boards.* *This issue is relevant also in the various future User Communities and Business/Adoption Models of MARISA.*
(MARISA-T1) Provide transparency and proper functionalities to help estimate the quality, reliability and validity of various data to be used. Code this information for the end-user to help her in the decision making.	*Essential Activity* *TECH WP3-WP5*	*This requirement is translated into several requirements in the technical baseline. Specific KPIs have been defined to monitor the fulfilment of the functionalities during the validation. Rules can be configured by the users. Refers to technical documentation (D3.x, D4.x, D5.x)* *MARISA_UR_GEN_55, MARISA_UR_GEN_60 various MARISA_UR_DF1 requirements* *The AI-checklist will also be used in order to investigate the transparency issues in MARISA.*
(MARISA-U2) Operational decisions shall never be made by a computer, not even the most efficient one: it must always be a human who makes the final decisions. MARISA can only assist in operational decision making, by providing information to the end-user/decision makers. The end-users must be informed regarding these liability issues in the training material.	*Essential Awareness* *TRAIN WP8*	*The users will be always in the loop, the toolkit will support decision making and planning being the final decision lies on the end-users. This is clearly explained in the training and user manuals*

(MARISA-B5) Organizational activities concerning Data Protection must be applied as part of the governance model for each new implementation of MARISA. Conducting a light PIA before the implementation is essential.	*Essential Activity* *BM/GM WP8*	*The final ethics deliverable D2.13 provides basic guidelines the organizational activities. These are to be embedded in MARISA exploitation/business modelling and in training material. See also MARISA code of conduct in D2.13.*

CONCLUSIONS

It should be evident that ensuring the proper implementation of ethical requirements is essential for any project. In spite of this, ethical compliance has long been near synonymous with proper research ethics, other important dimensions having been left with more or less an anecdotal status. The problematic nature of such a narrow perspective is often particularly accentuated in cases where a project's subject matter falls under a security topic. The RANGER project provides an illustrative example of this: when technological advancements lead to an increased surveillance capacity for authorities (in this case in the form of novel over-the-horizon radars), so do the moral and legal duties to act against ill will and to help those in distress; with great power comes great responsibility. Furthermore, the developed technology can fundamentally change practice and customs: the moral division of labour can be altered, a change that calls for holistic ethical considerations.

To answer to these challenges, we have attempted to develop a systematic framework for identifying ethical aspects from a more comprehensive viewpoint than that provided by the traditional science and research integrity perspective. One goal is to help developers and practitioners of technological innovations to turn these aspects into tangible sets of ethical requirements to be addressed during all phases of the project and on all layers of the solution being created.

The critical thing to realise is that ethics is not about declaring principles. Rather, it is intertwined in every aspect of a project and beyond, from the proper development of products and services, to their use, and all the way up to business and governance processes.

ACKNOWLEDGMENTS

The research leading to these results has received funding from the European Commission's H2020 research and innovation program, under grant agreement no 700478 (RANGER), and grant agreement no 740698 (MARISA).

REFERENCES

[1] Wright, D. and Raab, C. D., "Constructing a surveillance impact assessment," Computer Law & Security Review 28(6), 613- 626 (2012).
[2] Jeandesboz, J., "Beyond the Tartar Steppe: EUROSUR and the Ethics of European Border Control Practices," In Burgess, J. P. and Gutwirth, S. A. (eds) Threat Against Europe? Security, Migration and Integration, VUBPress, Bruxelles, 111-132 (2012).
[3] Crépeau X., Report of the Special Rapporteur on the human rights of migrants, François Crépeau - Regional study: management of the external borders of the European Union and its impact on the human rights of migrants, UN Human Rights Council 24 April 2013, A/HRC/23/46.
[4] Leese, M., Lidén, K., & Nikolova, B., "Putting critique to work: Ethics in EU security research," Security Dialogue, 50(1), 59–76 (2019).
[5] Zwart, H., Landeweerd, L. & van Rooij, A., "Adapt or perish? Assessing the recent shift in the European research funding arena from 'ELSA' to 'RRI'," Life Sci Soc Policy (2014) 10: 11.
[6] Esteves, A. M., Franks, D. and Vanclay, F., "Social impact assessment: the state of the art," Impact Assessment and Project Appraisal, 30(1), 34-42 (2012).