Stitching lacunas in open source intelligence – Using Ethics to fill up legal gaps

Milaj-Weishaar, Jonida; Mifsud Bonnici, Jeanne

Published in:
Illyrius - International Scientific Review

Publication date:
2022

Stitching lacunas in Open Source Intelligence – Using ethics to fill up legal gaps

Dr Jonida Milaj – Prof Dr Jeanne Pia Mifsud Bonnici[1]

1. Introduction

OSINT or open source intelligence is intelligence gathered from data that are publicly available in open sources, among which one can mention the internet, social media, newspapers, radio and television, government reports or even professional and academic literature. As technology develops, the volume of available data increases making organisations and individuals to rely for their intelligence purposes often solely on OSINT rather than on private and classified information. Economic evaluations as well as the easy accessibility and availability of OSINT tools and techniques has influenced the use of this method. Furthermore, there is a general believe that because the first material, the data, are publicly available, there should be no concerns about compliance with any data protection or privacy rules.

The Open Data Directive adopted in June 2019 addresses only data held by public sector bodies in the Member States, at national, regional and local levels, such as ministries, state agencies and municipalities, as well as organisations funded mostly by or under the control of public authorities. It focuses on the economic aspects of the re-use of information rather than on access to information by citizens and, encourages Member States to make as much information available for re-use as possible. The scope of this law is thus limited and it does not cover the use of OSINT for open data in social media platforms. Since there are no specific rules applying to OSINT at European level, for protecting the fundamental rights to privacy and data protection of individuals, the general legal framework becomes crucial.

This paper takes a legalistic and human rights approach and analyses in how far the use of open data from social media platforms for intelligence purposes is compatible with the fundamental rights of individuals and especially with data protection and privacy rules in the European Union.[2] As with many responsible data

[1] The authors are part of the Security, Technology and e-Privacy (STeP) research group, University of Groningen, Groningen, The Netherlands. This research was conducted in the framework of the MIRROR project that has received funding from the European Union's Horizon 2020 Research and Innovation Action Program under Grant Agreement No 832921.

[2] For the distinction between OSINT and SOCMINT please see: <https://privacyinternational.org/explainer/55/social-media-intelligence> accessed 5 May 2021.

concerns, legal compliance is just one part of a much bigger picture and it often forms the lowest rather than the highest bar one should strive for. In this light, the paper further elaborates on ethical concerns that are behind the legal rules and analyses how to use ethics for filling any gaps in the laws and ensure the protection of the fundamental rights of the individuals.

After this short introduction, in section 2 more information on the way OSINT operates is given. Section 3 analyses the compliance of OSINT with data protection and privacy rules. Section 4 goes one step further in identifying ethical concerns in the use of OSINT and elaborates upon the role of ethics in addressing these concerns. In section 5 a number of recommendations on how to use ethics for filling in legal gaps in OSINT are presented. The concluding remarks are presented in section 6.

2. Understanding OSINT and the information used

OSINT techniques allow for access to open-source data for anyone, anywhere and with any legal means. Those means can include tools and knowledge that are freely accessible and free in use. Thus, the OSINT 'miner' or user can range from an average enthusiast behind a computer to global intelligence agencies.

However, in literature OSINT is often referred to as a grey area. The reason for this is that while on one side OSINT can be a seemingly open, free and transparent system without legal restraints, on the other side it is also a system increasingly used by intelligence agencies with the aid of special techniques. The later questions the extent of the legal restraints on the techniques and on their use.[3]

In order to analyse the legality of OSINT uses, first the type of information used by an agency or individual must be identified. This is normally divided into four categories:

- White information;
- Grey information;
- Black information;
- Non-existing information.

White information is completely available to the public, is open and according to estimates, amounts to 90% of all data used in intelligence. Grey information is distinguished from white and black information because, even if not completely available all that is required to access it is to find the correct communication channel (e.g., universities, corporations or government institutions). You need to be a member of an organization in order to access this information but you do not need other special qualities (for example getting access to the archives of the city or becoming a member of a specific library in order to learn if a book is available). Black or classified information is not freely of semi-freely available and it is retrieved through covered activities. According to estimates, it constitutes only around 0,9% of all information used in intelligence activities.[4] The last category, non-existing information refers to information that cannot be found or accessed as such in open, semi-open or closed sources but it is deduced on the basis of other existing information.

[3] Gašper Hribar , Iztok Podbregar and Teodora Ivanuša, 'OSINT: A"Grey Zone"?' (2014) 27(3) International Journal of Intelligence and CounterIntelligence 529.
[4] Hribar, Podbregar and Ivanuša (n 3).

The legality of OSINT practices can thus be analysed based on the type of information used. This paper focuses only on the first category of information, white information, and only with regard to social media. White information on social media is freely accessible and available without the need of, for example, creating fake accounts or presenting fake credentials. In a more thorough legal research of privacy expectation in intelligence gathered by social media in the United Kingdom, Edwards and Urquhart argue that, currently, no privacy protection is given to white information.[5] Identifying the same problem and making a further step to offer some legal restraints to OSINT, Koops, Hoepman, and Leenes propose an integration of privacy by design in the systems of OSINT.[6] Both of these approaches indicate how current legal restraints to OSINT are lacking and require broader normative reasoning, especially given the very high percentage that the use of this technique based on white information occupies in intelligence activities. The following section will analyse how OSINT focusing on white information gathered from social media is considered in light of data protection and privacy rules in the EU.

3. Data protection and privacy concerns

As seen in the previous section, OSINT operates by harvesting open data that are freely available. These can be text, images, audio, etc. Being openly accessible though, does not change the qualification of some of these data as personal ones.[7] The public accessibility of the data makes many actors assume that using these data does not raise any responsibilities for addressing lawful data processing[8] or privacy criteria. For not falling into this fallacy, we will analyse below if the use of open data in a OSINT context complies with the legal rules. First data protection and then privacy concerns are addressed.

i) Data protection

There are two main data protection laws operating at EU level. The GDPR and the Police Directive.[9] Since this paper focuses on the use of open data in general and on OSINT practices available to individuals or organisations, without limiting our research to intelligence agencies or law enforcement activities, the GDPR is the relevant law. The Police Directive is not directly applicable to this general research given its limited material and personal scope of application.[10]

---

[5] Lilian Edwards and Lachlan Urquhart, 'Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence?' (2016) 24 International Journal of Law and Information Technology 279.

[6] Bert-Jaap Koops, Jaap-Henk Hoepman and Ronald Leenes, 'Open-Source Intelligence and Privacy by Design' (2013) 29 Computer Law & Security Review 676.

[7] Regulation (EU) 2016/679 0f the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (GDPR) [2016] OJ L119/1, art 4(1).

[8] Art 5 GDPR.

[9] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and the repealing of Council Framework Decision 2008/977/JHA (Police Directive) [2016] OJ L119/89.

[10] Art 1(1) Police Directive.

'Personal data' are defined in the GDPR as any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person, on the other side, is the one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Only a complete and irreversible anonymization of the data used would make the GDPR inapplicable. The GDPR does not regulate explicitly the use of open source data. However, as long as these data fall within the definition of personal data the general legal framework applies.[11]

For complying with the data protection framework, attention must be paid to the principles of lawful data processing established in article 5 GDPR, namely: (a) lawfulness, fairness and transparency; (b) purpose limitation; (c) data minimization; (d) accuracy; (e) storage limitation; (f) integrity and confidentiality; and (g) accountability. Furthermore, for personal data to be processed, compliance with the principle of lawfulness is very important. This principle requires compliance with one of the conditions established in article 6 GDPR.

For open source data collected from the social media, the condition of consent for processing the data cannot be established. Making personal data available does not automatically qualify as giving the consent to whomever has access to these data to process them as deemed necessary. Furthermore, we are all aware of the fact that often our personal data online are not made available from us, but from others. In this situation, processing of open data for research purposes in academia, for example, can be considered as lawful under the justification of performance of a task carried out in the public interest.[12] Open data processed for other OSINT purposes must comply as well with one of the conditions prescribed in art 6 GDPR.

In addition, some of the processed data might qualify as sensitive ones.[13] A personal image, for example, might reveal the religion of the data subject or his ethnic origin. Such sensitive information might also be part of posts data subjects have made in social media platforms.[14] According to the GDPR, processing of sensitive data should not take place unless falling under specific situations for which such processing can be justified. The justification of article 9(2)(e) GDPR on data that are made manifestly public needs to be considered in a restrictive way and always in combination with the fulfilment of the conditions for lawful data processing in art 6 GDPR. In the absence of a clear definition and understanding of the limits of use for data made manifestly public,[15] the protection of the rights of individuals should prevail. As a result, any processing of open data that qualify as personal data must comply with the data protection regime in the EU.

---

[11] C-73/07 *Satakunnan & Satamedia* EU:C:2008:727, paras 46-49.
[12] Art 6(e) GDPR.
[13] Under the category of sensitive data fall personal data that have the potential to reveal the racial or ethnic origin of the data subject, his political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
[14] Art 9(1) GDPR.
[15] Case T-320/02 *Esch Leonhardt v ECB* EU:T:2004:45; Edwards and Urquhart (n 5).

ii) The right to privacy

While the processing of open personal data needs to comply with the legal rules, OSINT is intelligence that derives from the analyses of such data. The information obtained may go far beyond what the individuals have made public and thus severely interfere with their private sphere.

The right to privacy as defined in article 8 ECHR and article 7 of the EU Charter of Fundamental Rights protects the private sphere of the individuals which seems from the wording of the articles as projected mainly in private spaces (private and family life, home and correspondence). When someone exposes himself in a space that is open to the public, including also the cyberspace, he creates the possibility to be visible to others whom have a right to observe what goes on around them. It is, however, one thing to be seen in public and another one to be tracked. The protection of the private sphere of the individuals would not be complete if data collected and recorded about their activities in public spaces are not covered.[16]

In Europe, the extension of the private sphere of individuals to the public space is to be found in the jurisprudence of the European Court of Human Rights. The capture of an event changes its nature from a simple observation to a record and, it is the systematic or permanent storage of data collected in open spaces as well as their compilation, processing, use or disclosure that makes these data fall under the protection of the right to privacy.[17] In *P.G. and J.H.* the European Court of Human Rights dealt with the scope of the right to privacy in public spaces establishing that: "*Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain*."[18] The same Court confirmed in *Perry* that the right to privacy exists also outside a person´s home or private premises.[19] While a simple viewing of activities, even if aided by technology, without any recording is considered as compatible with the right to privacy,[20] the situation changes as a result of new technologic developments which systematically or permanently record the data. Even though the above reasoning was designed for the physical world, the same logic can be easily extended to cyberspace and activities that individuals perform in social media.

Furthermore, individuals might still have a reasonable expectation of privacy for activities taking place in public. The reasonable expectation of privacy is to be seen mainly as a subjective element, linked with the feelings and expectations of an individual.[21] In *Rotaru* for example, the ECtHR recognized that an expectation of privacy followed by the right to protect it exists when a government agency systematically collects and stores personal information, even when this information is public.[22] Furthermore, in *Perry* the ECtHR reasoned that an individual has a reasonable expectation of privacy when could have not been reasonably expecting the

[16] Teresa Scassa, 'Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy' (2009) 7(2) Canadian Journal of Law and Technology 193.
[17] Sjaak Nouwt, 'Reasonable expectation of geo-privacy?' (2008) 5(2) SCRIPT-ed – A Journal of Law, Technology and Society 375.
[18] *PG and JH v The United Kingdom*, ECHR application no 44787/98, 25 September 2001, para 57.
[19] *Perry v The United Kingdom*, ECHR application no 63673/00, 17 July 2003, para 37.
[20] *Perry v The United Kingdom* (n 19), para 38.
[21] Tomas Gomez-Arostegui, 'Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations' (2005) 35(2) California Western International Law Journal 153.
[22] *Rotaru v Romania*, ECHR application no 28341/95, 4 May 2000, para 43.

use of technology for scopes beyond the normal foreseeability of their use.[23] The same reasoning would apply also with regards to OSINT since individuals using social media without the proper privacy filters are not expecting that the data will be harvested and processed for OSINT purposes. As a result, the right to privacy as established in article 8 ECHR and article 7 of the European Charter must be protected also in those cases in which data are made public from individuals themselves.

4. Ethics and Ethical concerns of OSINT practices

It is a well-known fact that technology is developing at a fast pace and answering the legal challenges proves difficult. Adopting proper legislation requires time and ethics are therefore of paramount importance as they can be considered as "soft law" even in absence of an ethical framework *stricto sensu* to respect. Even in a modern society governed by the rule of law unwritten laws keep existing and regulating behaviours.[24] Ethics goes far beyond the laws to consider ways of behaviour that would not cause harm to others.[25]

There are a number of legal instruments in the EU that have incorporated ethical provisions and that have contributed to raising some ethical concerns to the level of legally binding provisions. Some of these can be found also in the GDPR as well as in the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union (CFR). The concept of human dignity, for example, present in the GDPR in article 88 and in Recital 4, is interpreted as containing "a very general ethical reference" when it says that "[t]he processing of personal data should be designed to serve mankind."[26] The concept is also found in art 1 CFR.[27] The ECHR and the CFR are a source of ethical norms when they empower individuals to control the way information about them is collected and used via the right to privacy[28] and the right to data protection.[29]

Moreover, according to the Ethics Guidelines for Trustworthy Artificial Intelligence from the European Commission, trustworthy AI should be respecting ethical principles and values.[30] They emphasise the need for transparency and accountability that is also present in the GDPR,[31] as well as the criteria for consent,

---

[23] *Perry v The United Kingdom* (n 19), para 41.

[24] This stems from Aristotle's Nicomachean Ethics in which he distinguishes between "the legal or conventional justice (that is achieved by applying legal rules) and natural justice (which remains valid everywhere, hence independent of particular laws)" - see Georgeta-Bianca Spîrchez, 'The relation between ethics and law', (2016) 1 Fiat Iustitia, 189.

[25] Ferdinand Curtney French 'The Concept of Law in Ethics' (1893) 2(1) The Philosophical Review 35.

[26] Hielke Hijmans and Charles Raab, 'Ethical Dimensions of the GDPR' (2018) in: Mark Cole and Franziska Boehm (eds) *Commentary on the General Data Protection Regulation* (Cheltenham: Edward Elgar, 2018) 2, available at <https://ssrn.com/abstract=3222677> accessed 30.3.2021.

[27] Art 1 CFR "Human dignity is inviolable. It must be respected and protected. "

[28] Art 8 ECHR and Art 7 CFR.

[29] The right to data protection is not explicitly mentioned in the text of the ECHR but the European Court of Human Rights has based it on the 'general' right to privacy in several decisions. See for example: *Leander v Sweden*, ECHR application no 9248/81, 26 March 1987, para 48; *Kopp v Switzerland*, ECHR application no 23224/94, 25 March 1998, para 53; *Amann v Switzerland*, ECHR application no 27798/95, 16 February 2000, para 69.

[30] AI HLEG, 'Ethics guidelines for trustworthy AI' [2019] available at <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai> accessed 13.3.2020.

[31] See for example art 57(1)(b) GDPR.

transparency, diversity, non-discrimination and privacy.[32] The principle of fairness is also considered a component of ethics. As such, article 5(1)(a)) GDPR "elaborates this and associates it with transparency" although this is not agreed by everyone.[33]

While there is no legal obligation to comply with ethics apart from those mentioned, this does not mean that engaging in OSINT, one should not respect them. The development of technology is faster than the adoption of legal responses and ethics are therefore of crucial help as they play the role of 'soft law' standards. In the same way OSINT has to comply with the rights to privacy and data protection from the beginning, it also must respect the ethical safeguards which have reached the level of legally binding provisions as well as other ethical concerns not legally binding. The rationale lies in the nature of the EU itself. It is governed by the rule of law enshrined in Article 2 of the Treaty on European Union, which is a prerequisite for the protection of all fundamental rights in the EU.[34] Especially, the rule of law in the EU aims at strengthening mutual trust between actors, in particular between citizens and governments. Even if ethics are not law, observing them contributes to pacifying relations in the EU. Moreover, ethics can often be found in the legislation since the role of law often consists in making ethical choices.

The main ethical concerns identified when engaging in OSINT practices are explained below.

i) Dignity and autonomy of individuals

OSINT practices mean that there is a risk that people are associated to a mere set of data and that entails a risk for their autonomy as human beings and for their dignity. Collecting data from individuals without informing them about this activity might emphasise the idea that data speak for the individual and that there is no need to get the information directly from them since data already does it for them. Thus, getting data about individuals without their involvement can be problematic regarding their autonomy and dignity as human beings.

ii) Trustworthy data, dignity and autonomy

Furthermore, it is problematic to collect data retroactively since past data potentially does not reflect what the person thinks and is now, and the same applies concerning the group they belong to. This concern would rise in case OSINT engages in individual profiling. This is linked to the question of how can we be sure that the data is trustworthy. Indeed, deeming a person to have kept the same ideas and opinions over the years can be harmful for her or his right to autonomy and therefore damage the human dignity. Thus, the period time should be considered when harvesting data and machine learning should be designed in a way that does not reach too far in the past and adopt a dynamic approach regarding people's development.

---

[32] AI HLEG, 'Ethics guidelines for trustworthy AI' [2019] available at <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai> accessed 13.3.2020.

[33] Hielke Hijmans and Charles Raab, 'Ethical Dimensions of the GDPR' in: Mark Cole and Franziska Boehm (eds.) *Commentary on the General Data Protection Regulation* (Cheltenham: Edward Elgar, 2018) 2.

[34] Dimitri Kochenov and Laurent Pech, 'Upholding the rule of law in the EU: on the Commission's 'pre-article 7 procedure' as a timid step in the right direction' (2015) Working Paper, EUI RSCAS, 2015/24, Global Governance Programme-164, Global Economics.

iii) Discrimination

This issue of discrimination can be found regarding the origin of the data that is analysed. Whose data are processed and how are specific categories of individuals targeted? It can be a problem to decide to focus on a specific national group or on a certain gender or age. Issues relating to autonomy can be seen with the risk that the data found on those grounds will help making shortcuts about people. In particular, there is a risk that it leads to individual or group profiling.

iv) Risks of biases, creation of stereotypes and discrimination

Furthermore, the data cannot speak for itself since it is something intangible and that does not have an existence on its own. It is a mere emanation of a human being. To understand what is really behind the data, it must necessarily be interpreted. As a result, risks of biases from actors appear. The ethical dilemma raises concerns on how far one can trust a computer program to grasp the opinion of someone based on available data or even of a whole population. Careful consideration must therefore be given to the way computers potentially reproduce the biases that already persist within society. That problem is linked to the extent to which computers can be trusted. Who will decide whose data is harvested is a key question. Moreover, data mining processes often rely on simplistic stereotyping of the target, the outcome of such searches may also be discriminatory consequently.

v) Chilling effects

The use of OSINT techniques can also produce chilling effects in the society. The consequence of using such technology can be a change in the behaviour of individuals: knowing that their feelings, opinions, ideas are analysed, they might decide to auto-censor themselves to avoid the screening of their social media. This can have chilling effect on certain human rights, notably freedom of expression. Risks of biases and shortcuts resulting from a look at the group and not at the individuals alone can be harmful to the perception other people have of that group. Discrepancies can arise from a simplistic analysis of individual's data while they do not necessarily reflect his opinions, and even less those of a whole group. Wrong ideas concerning a certain group of origin can be extremely harmful.

5. Introducing ethical safeguards

It is often said that laws are nothing more than codified ethics and that all laws are designed with ethical concerns in the background.[35] But a problem that we face nowadays is that the laws lack far behind any technological development. In the absence of specific legal regulation, the general legal framework applies but, as it was seen in the previous section, the later does not address all the potential ethical concerns that might arise by the use of specific technologies. As a result, the ethical concerns remain unaddressed with the risk of being projected into ineffective safeguards for the fundamental rights of the individuals.

[35] See Giovanni Buttarelli, 'An ethical approach to fundamental rights' (1 December 2016, EDPS Blog) <https://edps.europa.eu/press-publications/press-news/blog/ethical-approach-fundamental-rights_fr> accessed 1.12.2019, mentioning a quote often attributed to Mahatma Gandhi.

Since compliance with the legal rules often forms the lowest bar rather than the best practice one should strive for, it is important not to limit oneself to the legal aspects of the use of a new tool or of OSINT technology but to address also all potential ethical concerns at the upfront. Ethics goes far beyond the laws to consider ways of behavior that will not cause harm to others. In case of OSINT practices, the main harm to the individuals is the interference with their fundamental rights. Basing behavior on ethics would mean to safeguard the fundamental rights to privacy and data protection in the presence of legal lacunas.

The previous section identified a number of ethical concerns and highlighted their nature. Even though these concerns escape the current legal regulation and ethics are not *per se* legally binding, it is still possible to design a course of action, linked to their nature, in order to address them without falling in the fallacy of ethics washing.[36] Firstly an upfront, we can raise the awareness of designers and users of OSINT technologies about potential ethical concerns to help in addressing these issues at an early stage.

Secondly, we can add ethical concerns to a necessity and proportionality assessment before the introduction of any OSINT technologies. However, given the fact that these principles lack a normative value the risk remains that adding ethical concerns to the equation will not help. Ethics also lack in normative value and will only add some smoke to the already existing gray area of the application of the principles of necessity and proportionality without addressing the problem.

Thirdly, we can link any ethical concerns, depending from their nature, with pre-existing legal requirements. If ethical concerns are linked with the design of the tool, for example, we can address these concerns at an early stage and make them part of the data protection by design and default assessment. Since data protection by design is already a requirement of the data protection framework, we can add ethical concerns to such an assessment and address them to an early stage. We can extend any data protection impact assessment methodologies that will be undertaken to cover also ethical concerns. We would thus design not only a data protection impact assessment but also integrate it with an ethical impact assessment. In the same line, if the ethical concerns derive from the way of operating of the tool, we can identify the concerns and compile them in codes of ethics as well as in approved codes of conduct that will be obligatory to comply with and prescribe legal consequences for the users of the OSINT technology. In this way, we would be able to address legal concerns that do not yet find protection in the laws and at the same time fill in lacunas that we currently find in the legal framework regarding OSINT. Below follow a number of suggestions on how to extend existing legal requirements for addressing ethical concerns:

a) Ethics by design

While the concept of 'data protection by design' contained in the GDPR obliges controllers of personal data to implement technical and organisational measures, at the earliest stages of the design of the processing operations, to safeguard data

[36] Ben Wagner, 'Ethics as an Escape from Regulation: From ethics-washing to ethics-shopping?' in Mireille Hildebrandt (ed), Being Profiling. Cogitas ergo sum (2018, Amsterdam University Press) 84.

protection principles right from the start,[37] the concept of 'ethics by design' has emerged in parallel. In a similar fashion, it requires the introduction of an ethical analyses and safeguards from the start of a OSINT project. In this way, data protection concerns are extended with ethical ones.

b) Necessity and proportionality requirements

To ensure the respect of autonomy and human dignity, the principles of necessity and proportionality are of great relevance. Especially, they must give answers regarding the time span of data collection. How far back in time personal data is collected determines whether these principles are respected. Indeed, the older the data is collected and analysed, the lesser autonomy people are given. Moreover, ethical challenges can be identified regarding the volume of data that is processed. Depending how much is collected and processed, ethical concerns could grow higher or decrease.

c) Transparency

Other ethical safeguards pertain to transparency. As much as possible OSINT must seek to be transparent with whomever is involved in the research conducted. This finds echo with the right to information in the GDPR according to which there is "no privacy without transparency." Derogations to this right are included in article 89 GDPR which allows, for example, derogations from Article 15(3) in case the data are processed for scientific purposes.

d) Accountability

For scholars "[t]o ensure accountability, decisions must be derivable from, and explained by, the decision-making algorithms used."[38] Therefore, accountability is closely linked to transparency. However, since machines are assumed to be incapable of moral reasoning, "accountability must remain on the humans – those who designed or programmed the machine, or those who customised and deployed it, or those who use it." Predictive big data analytics should also not be used in a way that leads to predictions which replace in turn human expression. They should keep the human being at the centre at all times.

e) Acknowledging biases

In order to avoid the reproduction of stereotypes, the designed tools and agents dealing with personal data should develop a methodology that avoids making hasty conclusions when data is analysed. Stereotypes, whether they are on national, ethnical, gender, political or any other relevant ground must be considered; machines as well as humans should pay great attention to, first, identify potential stereotypes they may be dealing with, and secondly, to avoid reproducing them. This issue is

[37] Art 25 GDPR.

[38] Virginia Dignum, Louise Dennis, Marlies van Steenbergen, Christina Baroglio, Tristan de Wildt, Matthijs Smakman, Raja Chatila, Maurizio Caon, Juan Pavón, Matteo Baldoni, Roberto Micalizio, Malte S. Kließ, Leon van der Toree, Gonzalo Génova, Serena Villata, Galit Haim, Stefano Tedeschi, Maite Lopez-Sanchez, Marija Slavkovik, 'Ethics by Design: Necessity or Curse?' (2018) AIES 18 - Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society, 60.

linked to the problem of unfair inequalities between people and the discrimination resulting thereof.

6. Conclusions

As it was seen above, there are both legal and ethical concerns with which the users of OSINT need to comply. The fact that the data used for OSINT are in the open space does not change their qualification as personal data and the application of the legal rules. Furthermore, the use of these data might interfere with the private sphere of the individuals and thus the right to privacy of individuals needs to be safeguarded. As this paper argued, for the proper protection of the fundamental rights of the individuals one cannot limit himself to compliance with the legal aspects of the tool used and activity performed. Even the most perfect implementation of laws (that by nature are imperfect) would leave gaps that need to be filled, and ethics can be used for filling these gaps. Ethics go further than the legal rules in identifying potential concerns for the proper and effective protection of the rights of the individuals. Therefore, ethical concerns, even if not yet reflected in legal choices, need to be addressed at the upfront and a course of action linked with the type of ethical concerns identified needs to be designed.

In OSINT ethical concerns are linked especially to the dignity and autonomy of the individuals, to discrimination and prejudices as well as to chilling effects in the society. Addressing these concerns from the start of a OSINT project helps to safeguard the fundamental rights of the individuals in the presence of legal lacunas. Since ethics do not have a binding requirement in themselves, extending already existing legal requirements would contribute towards achieving the goal. In this way, ethics help to close the gaps between the standards set by the laws and the proper protection of the fundamental rights of the individuals. They contribute towards mitigating any disconnections between the laws and the technology.