ROXANNE Ethical, Legal, and Societal analysis: Fundamental Rights Aspects

ROXANNE

This project has received funding from the European Union's Horizon 2020 Programme under grant agreement n°833635. The document reflects only the authors' views and the European Commission is not responsible for any use that may be made of the information contained therein.

ROXANNE is a research project funded by the European Union that intends to combine new speech, text, video, and network analysis technologies into a new platform that will assist law enforcement agencies to identify criminals in organised crime investigations. A key part of this project is ensuring that the activities within the project, and the project results comply with ethical, legal, and societal standards. This is achieved through taking Privacy and Ethics-by-Design approaches to the research activities in the project that are investigating tools and methods to be incorporated into the new platform. To be able to fully engage in these approaches, partners from the project's ethics and legal team have conducted in-depth analysis into the ethical, societal, fundamental human rights, and applicable legislation (including data protection and rules concerning INTERPOL) aspects of the project, and the proposed platform. So that these analyses can be validated, the project's ethics and legal team are sharing a series of briefing papers with important stakeholders to gather feedback. A link to a survey will be provided separately where you will be able to share comments if you wish.

1. INTRODUCTION

Fundamental rights are an important consideration for the developers of security technologies, as there is significant potential for the rights of persons who are being investigated to be impacted using those technologies. It is crucial for legal compliance that technologies used in law enforcement situations are developed in such a way that they do not automatically violate rights, but can instead facilitate fundamental rights being respected and, potentially, fulfilled.

ROXANNE ethical and legal partners evaluated the relevance of different rights in the EU Charter of Fundamental Rights (EUCFR) for the project and focussed on analysing those that are most relevant to the ROXANNE project and platform. This document summarises the most relevant points from that analysis.

The applicability of the EUCFR is relevant to the potential use of the ROXANNE tools by law enforcement agencies (LEAs) 'when they are implementing Union law', as stated in Article 51(1). As the ROXANNE platform process data about people, we can expect that this would involve the domestic implementation of the Law Enforcement Directive (2016/680) which regulates the processing of personal data by LEAs. As the EUCFR is not implemented as broadly as other human rights documents, the ROXANNE partners took a comparative approach to fundamental rights, including analysis from other treaties where this would further their understanding. The EUCFR somewhat already includes this under Article 52(3), which provides for parallels to be drawn from the European Convention on Human Rights to the European Union Charter regime.

So that issues raised at the project stage are not ignored, the following analysis also incorporates a 'Business and Human Rights' approach. This means that the fundamental rights implications present in the project are also considered even where those concerns relate to private actors in the consortium, who do not legally have human rights obligations.

2. FUNDAMENTAL RIGHTS ANALYSIS

The analysis of each right offered below first defines each right that is thought to be relevant to ROXANNE, and then explains the nature of the right. Next, the relevance of the right to the development and use of the project are explained.

Article 3 – Right to the integrity of the person

This right is defined as:

> *'1. Everyone has the right to respect for his or her physical and mental integrity.*
>
> *2. In the fields of medicine and biology, the following must be respected in particular:*
>
> - *the free and informed consent of the person concerned, according to the procedures laid down by law,*
> - *the prohibition of eugenic practices, in particular those aiming at the selection of persons,*
> - *the prohibition on making the human body and its parts as such a source of financial gain,*
> - *the prohibition of the reproductive cloning of human beings.'*

This article relates primarily to health,[2] including mental suffering, anxiety, indignity, and humiliation.[3] This right is based upon Article 26 of the European Convention on Human Rights and Biomedicine that can be restricted in the interest of public safety, prevention of crime, the protection of public health, or for the protection of the rights and freedoms of others.

Relevance to the project

During the project, this right has relevance to the use of human participants in research activities. Although paragraph (2) of this Article explicitly refers to the fields of medicine and biology, it is worth observing the legal rules therein due to the involvement of human participants in ROXANNE.

Human participants are volunteers who can withdraw at any time, are not forced or pressured to participate in any way. The ROXANNE partners do not expect that participants will be subject to anything that could cause them mental[4] or physical harm.[5] Participants are provided with all relevant information and can make a free choice whether or not to participate. Thus, there would not seem to be any infringement on the integrity of participants.

Relevance to use

The ROXANNE platform is designed to be used by LEAs to analyse data during organised crime investigations. Consequently, paragraph (2) of this Article is not applicable. Further, as, data-analysis does not require physical contact between LEA officers and suspects, use of ROXANNE tools is unlikely to have any direct impact upon the physical integrity of persons.

In terms of mental integrity, it is not unimaginable that a person investigated by LEAs might find out that they were under surveillance if they are informed of this during the court process. This could, potentially, lead to feelings of mental suffering, anxiety, indignity, and humiliation.[6] It is important to note that the individual technologies researched in ROXANNE are already available to LEAs for lawful data-analysis, and their inclusion in the ROXANNE platform does not create any additional inherent risk of violating this right. The European Court of Human Rights requires states to implement legal frameworks with enforcement mechanisms to protect the psychological integrity of persons.[7] As the intended market for ROXANNE is in Europe, the expected end-users will likely have already implemented such measures. If not, then they should be put in place before using ROXANNE. In any case, it is likely that any interference with this right could be lawful in situations where placing a suspected criminal under surveillance is necessary and proportionate to investigate or prevent criminality.

Article - 6 Right to liberty and security

This right is defined as: *'Everyone has the right to liberty and security of person'*. It has the same meaning and scope as Article 5 of the European Convention[8] by virtue of Article 52(3).

This article relates to the ability of persons to freely move in physical space.[9] Although the form of a deprivation of liberty should be interpreted widely,[10] it is focussed on the right not to be detained arbitrarily.[11]

Relevance to the project and use

It is unforeseeable that a research participant or colleague would be physically detained in any way as part of their engagement with the project. As such it is not relevant to the project.

In terms of use, it is also difficult to consider that the use of a platform intended to analyse surveillance data could have a direct effect on the ability physical liberty of a person. However, the effect of surveillance and LEA data analysis could affect the liberty of suspects. For example, if someone were to be aware they were at risk of having their data analysed by a ROXANNE-like system, then this would likely create 'chilling effects' where people change their behaviour owing to the (risk of) coming to the attention of LEAs as, in order to avoid punishment, the only 'rational' option is to follow the expectations of the LEA.[12] Such concerns are relevant to the ROXANNE platform as people are likely to want to shield their associates whom they are in communication networks with. The manifestation of such effects could have significant impacts upon how much liberty people feel they have. For example, some people may stop exercising their liberty. However, even if people do feel constrained in their behaviours owing to (a risk of) being analysed by ROXANNE, the article relates to physical liberty only.

We can however anticipate a situation where outputs from such a data analysis platform contribute towards suspicion that an offence has taken place, thus leading to the arrest and detention and subsequent loss of liberty of a suspect. If the outputs of the platform and tools are false, erroneous, have been insufficiently tested, or are based upon poorly understood mechanisms, then the platform potentiality contributes to unlawful arrest and the deprivation of liberty. This creates an obligation upon the project to ensure high quality science, rigorous testing, and proper communication around the outputs of the tools and how they can be misleading.

Article 7 - Respect for private and family life

This right is defined as: *'Everyone has the right to respect for his or her private and family life, home and communications'*.

The meaning and scope of this right are the same as those in Article 8 of the European Convention (although 'correspondence' has been updated to 'communications'),[13] by virtue of Art.52(3) of the Charter. Consequently, the limitation on the right in the Charter correspond to those in the Convention:

'2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'

Owing to the nature of this right, it is seen to have two separate limbs: private life aspects and family life aspects. Clearly, the processing of speech, text, and video data gathered by surveillance can affect both aspects, and the use of network analysis could be used to infer information across both aspects also. As such, ROXANNE could pose a particular challenge to this right.

Regarding the private life aspect, it is interpreted widely and also relates to one's home life and communications. It is focussed upon protecting activities of a personal nature, such as names, personal identity, and one's home.[14] These data are protected whether or not they have been processed.[15] This has links with the family life aspect as a person's name provides familial information.[16] Further, the private life aspect includes professional life as far as one's professional life is also part of one's home life.[17] For example, where one's home is also one's business premises.[18] The family life aspect is interpreted widely.[19] It is focussed on gender equality,[20] children's rights,[21] free movement, immigration, and asylum.[22]

Relevance to the project

The work of the ROXANNE project does not seem to raise any of the issues mentioned in Article 7 for colleagues or research participants as there is no expected interference with their private or family lives.

Yet, privacy issues do arise with the potential processing of data from real closed cases in order to test a prototype ROXANNE platform. If this happens, only lawfully gathered data would be acceptable for use. Of course, gathering these data in criminal investigations is a situation where respect for a persons' private and family life is clearly relevant. Thus, in order for it to have been gathered in compliance with this Article, any such surveillance data would need to have been collected in accordance with domestic law, and for it to have been necessary for one of the limitations provided in paragraph 2 to apply; in the case of ROXANNE, this is most likely to be 'for the prevention of disorder or crime'. Where this is the case, the infringement on the private and family lives of persons during an investigation is not arbitrary and the Article is complied with.

The re-using of surveillance data for research purposes would seem to be a separate situation where there is potential for infringing upon the respect for private and family life. Data gathered by surveillance is, by its nature, sensitive, and so all processing activities of it seem to raise a risk of infringing upon this right. Thus, in order for the processing of these data in the ROXANNE project to not violate Article 7, the same test as mentioned in the previous paragraph could be applied.

For such processing to be in conformity with domestic law, it must be processed according to applicable data protection legislation, i.e. the GDPR and the relevant national implementing legislation. By contributing to a project building new tools to assist in fighting organised crime and terrorism, such processing clearly contributes to the 'prevention of disorder or crime', and so this

part of the test is also met. In terms of whether these activities are necessary in order to prevent disorder or crime, the European Court has stated that there must be a 'pressing social need'[23] as understood by each state within a margin of appreciation.[24] The ROXANNE project responds to the difficulties experienced by LEAs in large organised crime investigations, and potentially solving or reducing these difficulties would seem to meet a pressing social need. The fact that LEA partners are permitted by their governments to participate in projects such as ROXANNE indicates that their states view their participation as contributing to a pressing social need also. Consequently, any interference with an individuals right to privacy experienced through the use of their data in the ROXANNE project could in compliance with the right. Having said that, the 'need' for real closed case data must be evaluated. Partners need to consider if it would be possible to test the ROXANNE platform using data that is less sensitive and not from real closed cases.

Relevance to use

The potential for the use of ROXANNE to infringe upon a person's right to privacy would seem to be the same as any other tool used in the analysis of investigative data by LEAs: its use would need to be in compliance with domestic law and necessary for, and proportionate to, the prevention of disorder or crime. In the current situation, tools used for identifying persons in surveillance data are used separately from network analysis tools, and investigators can assess the need for both activities separately. As ROXANNE brings both technologies together, this creates a requirement that the platform does not automatically run data through both types of tools as it might be necessary only to use one. For example, it might be necessary to identify a suspected criminal in an investigation, but not necessary to map their communication network and further infringe the privacy of the individual and their acquaintances.[25]

In order to analyse surveillance data that includes persons other than the suspect, it must also be necessary to infringe on the privacy of those innocent persons. With network analysis, this could be a large number of persons and so it could be difficult to assess the necessity of infringing on the privacy of every person, and whether the test should be applied to each person individually or the data-set as a whole. It would be insufficient simply to extend analysis to the data of other persons because they are merely 'involved in a criminal offence',[26] indeed the European Court requires that precautions to protect persons who are incidentally recorded must be enacted in domestic law.[27] Thus, in order to be lawful, the extension of criminal network analysis to the associates of a suspected criminal must have a basis in domestic law, which is specific enough to so that the persons who could be subjected to surveillance could be determined.[28] End-users will need to provide their legal basis in national law in an electronic decision-making mechanism before they can engage in data processing.

Article 8 - Protection of personal data

This right is defined as:

> *'1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
>
> *3. Compliance with these rules shall be subject to control by an independent authority.'*

Paragraph 1 of this Article comes from Article 16(1) of the Treaty of the Functioning of the European Union. With regard to secondary legislation, the EU has developed a range of instruments relating to personal data. The most relevant of these are the General Data Protection Regulation (GDPR), and the Law Enforcement Directive (LED).

The Charter is unique in that there is no corresponding right to the protection of personal data under other human rights treaties. This is despite the fact that data protection legislation itself provides rights to data subjects for specific instances (e.g. access,[29] rectification,[30] erasure[31]).

However, in other human rights regimes, the protection of personal data is considered to form part of rights to privacy.[32] For example, in assessing data privacy, the European Court has considered: the nature of the data;[33] the privacy expectation of the person concerned;[34] access of the person concerned to data;[35] the presence of oversight mechanisms;[36] whether security measures have been put in place.[37] A case-by-case approach is taken by the European Court, and so the precise contours of how the protection of personal data is dealt with under the right to a private life can only be foreseen generally.

The right to protection of personal data in the EU Charter is not absolute, 'but must be considered in relation to its function in society.'[38] Limitations on this right are recognised under Art.52(1) of the Charter. They must be provided for by law, respect the essence of the right, and be proportionate, necessary, and meet legitimate objectives.[39] The same approach is taken in relation to personal data forming part of one's privacy in other human rights regimes. [40]

Relevance to the project

The processing of personal data in the ROXANNE project is subject to the GDPR. As such, processing that is in line with this, or national implementing legislation, is provided for by law. The essence of the right is respected by using anonymous or pseudonymous data where possible, and preferring to process personal data on the basis of consent. Processing of personal data in the project is proportionate to the aim of conducting scientific research as there will be no direct

effects created for data subjects, and nor will there be any combining of datasets with the intention to uncover highly-sensitive information about data-subjects. The processing of personal data in the project is necessary as it would not be possible to produce the intended algorithms without training them on personal data. Scientific research is a legitimate objective as, by its nature, it results in greater knowledge and advancement for society and in the case of ROXANNE, potentially contributes to the increased safety of citizens from organised criminal gangs.[41]

Relevance to use

The processing of personal data during potential use of the ROXANNE platform in criminal investigations within the EU would be subject to the Law Enforcement Directive. Consequently, processing that is in conformity with this Directive, and national implementing legislation, would be provided for by law. Whether processing of personal data by LEAs is necessary and proportionate to meet a legitimate objective will depend upon the context of the investigations that are taking place. However, the ROXANNE consortium intends that any exploitation of the platform that involves its sale will only take place to organisations and countries who respect applicable human rights law and do not abuse their powers; as such, the consortium assumes that end-users will comply with the law during their usage of the platform. The electronic decision-making mechanism will provide a functionality for users to attest that their use of the tool is in line with national legislation and operational procedures by giving an opportunity for end-users to provide details on authorisations from judges or senior officers, for example. The decision-making mechanism also provides an opportunity for end-users to record their justification for processing personal data to discourage fishing for evidence and to allow accountability and auditability of the use of the tool within the end-user organisation.

Article 11 – Freedom of expression and information

This right is defined as:

> *'1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.*
>
> *2. The freedom and pluralism of the media shall be respected.'*

Due to Article 52(3) of the Charter, the meaning and scope of Article 11 of the Charter are the same as Article 10 of the Convention. 'Expression' covers a range of actions beyond just speech,[42] including silence.[43] It applies whatever medium of communication is used, including oral, written, printed, and electronic forms.[44] Indeed, the freedom of expression 'applies not only to the content of the information but also to the means of transmission or reception since any restriction imposed on

the means necessarily interferes with the right to receive and impart information.'[45] As such, a speaker (broadly conceived) has a right to make information available a recipient has the right to receive that information.[46]

Relevance to use

In terms of the ROXANNE project, it is unlikely that anyone's freedom of expression could be infringed upon as partners engage in free an open discussion on consortium business. When it comes to the potential use of the platform, as a data-analysis platform, ROXANNE would not have a direct impact on anybody's freedom of expression. However, there is potential that chilling effects could be created if an individual fears that their speech data is (at risk of) being analysed by LEAs using a platform such as ROXANNE, and they do not express themselves in order to avoid being recorded and included in this analysis for fear of being identified as a criminal. The freedom of expression protects all expression of information, apart from hate speech and incitement of violence.[47] Thus, an individual could, potentially, not express themselves about a range of topics that they do not wish to be recorded expressing or identified from. Because such analysis would likely be covert, an individual has no way of knowing if their particular expression activity is under surveillance.

European Court has held that 'self-censorship' of one's own expression due to a fear of court proceedings can violate the freedom of expression where the proceedings were unnecessary.[48] Consequently, if a criminal self-censors their own expression due to a fear of court proceedings occurring as a result of their criminality, and those proceedings are necessary, then is unlikely that the freedom of expression would be violated. Indeed it is likely to be seen as a form of deterring criminals from openly engaging in criminality. As such, this type of interference with the freedom of expression is unlikely to be unlawful.

Article 12 - Freedom of assembly and association

This right is defined as:

> *'1. Everyone has the right to freedom of peaceful assembly and to freedom of association at all levels, in particular in political, trade union and civic matters, which implies the right of everyone to form and to join trade unions for the protection of his or her interests.*
>
> *2. Political parties at Union level contribute to expressing the political will of the citizens of the Union.'*

Pursuant to Article 52(3) of the Charter, the meaning and scope of the right under the Charter is the same as that under Article 11 of the Convention.

Generally, the freedom of assembly protects the right of people to peacefully gather and meet for

political,[49] social,[50] communal,[51] cultural,[52] or religious/spiritual purposes,[53] whether in private or public and whether static or as a procession/march.[54] 'Association' here means an affiliation with a group that has a common goal,[55] not merely sharing the company of, or mixing socially with, others.[56]

The ROXANNE platform itself, as a data-analysis platform, cannot be used to directly interfere with the freedoms of assembly and association held by citizens. However, owing to the potential for people to be identified from video and audio data by the ROXANNE platform, and for this to be linked with communications networks, the implementation of ROXANNE could, potentially, have a significant chilling effect on the freedom of people to peacefully assemble/associate where they fear that they themselves, or people they communicate with, could be subjected to surveillance for their activities with others. The intelligence analysis capacities enhanced by the platform would also enhance these capacities if they were used in an inappropriate manner (e.g., illegal surveillance and disruption of legitimate political activists) so would contribute towards the impact of activities that could directly interfere with freedom of assembly and association.

Relevance to use

As data processing in the project is for the aim of technology development, rather than creating any effects for data-subjects, it is unlikely that freedoms of association or assembly could be engaged during the project. In terms of use, there is potential for a significant chilling effect to be created if, by knowing about the ROXANNE platform, people believe that they are subject to (a risk of) having their data analysed and being identified by LEAs. This effect is likely to be increased, where people are concerned that LEAs will be able to find out who they communicate with using the ROXANNE network analysis tools, thus exposing their associates to potential LEA interest.

The paradigmatic example of chilling effects in relation to freedoms of assembly/association is of LEA actions, directly or indirectly, inhibiting the freedom of people to engage in political activities, such as protests or trade union activities. LEA interest in protests has been determined by the European Court to have a chilling effect even where that interest is temporary,[57] or later shown to be mistaken,[58] and where LEAs act unlawfully to ban a protest.[59] For the European Court, the potential for chilling effects to be detrimental to the freedom of assembly should be considered in terms of whether their actions are proportionate.

If, for example, people involved in political movements decline to attend legitimate protests or meetings due to, a risk of, their data being analysed by ROXANNE-like tools, their freedoms of assembly/association could have been infringed upon. The most obvious solution to this, of course, would be to not sell or provide the ROXANNE platform to LEAs who use their powers to stifle legitimate political activities.

However, as noted above, freedoms of assembly/association also extend to social, communal, cultural, and religious/spiritual gatherings. If, for example, a member of an organised crime group

knew that they were at risk of surveillance and so stopped engaging in social events in order to protect their innocent associates, could this be an infringement on their freedom of assembly? Engaging in social and cultural activities are an important part of people's lives. But they are not essential, and so the choice of someone to not engage in them in order to avoid potential surveillance would not seem to be a disproportionate effect. Whether this could even be considered relevant to the freedom of assembly would, of course, depend upon whether these acts are too distant from LEA activities to be infringed upon by the LEAs themselves. It is unlikely that LEAs could be held to have infringed upon a person's right to assembly where an LEA has no contact with an individual yet they decide not to attend social events due to a fear of being subject to surveillance or data-analysis.

Articles 21 to 26 – Rights to non-discrimination

The ROXANNE project solutions and activities may have implications on fundamental rights such as the broad principle of non-discrimination and in relation to specific diversity aspects related to gender, culture, age or physical characteristics. Therefore, in the development of the ROXANNE platform and its subsequent use, it is important to be aware of any potential diversity and non-discrimination rights repercussions.

Article 21 of the EU Charter of Fundamental Rights prohibits "any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation". Furthermore, the EU Charter of Fundamental Rights prohibits discriminatory treatment on additional grounds, safeguarding cultural, linguistics and religious diversity in Article 22, equality between men and women in Article 23, the rights of children (Article 24) and elderly (Article 25), as well as integration of persons with disabilities (Article 26). There are several issues related to non-discrimination that could arise across the ROXANNE project, and potential use of the platform.

Data bias

In the pursuit of the ROXANNE project's tasks and objectives, the consortium should ensure the respect of the general and specific provisions of the rights to diversity and non-discrimination throughout the different project stages and activities. First, at the research level, the project should understand what biases relating to gender, age, language or racial bias exist in the datasets used for the development and testing of the algorithms. Where multiple datasets are available, the project should select and use those with the smallest bias and where this is not possible we should identify other methods to minimise bias. Existing research[60] highlights the significant dangers related to ethnic profiling and other discriminatory treatments when authorities employ innovative technical solutions, such as facial recognition systems, that were constructed on biased dataset. Where it is not

possible to remove bias in training data, technical partners should consider how they can mitigate the effects of bias and whether there might be issues that end-users should be aware of.

End-user requirements

Secondly, when analysing and defining the applicable end-user requirements, fair, impartial, inclusive and equal treatment should be given to the needs expressed by stakeholders coming from different backgrounds, i.e. operational units, forensics, country/culture wise, gender wise, etc. Given the value of expert feedback in designing feasible, realistic ROXANNE solutions that overcome current investigative shortcomings, the project team emphasized the importance of expert guidance and insight from the earliest stage and will continue this to the development of the finished ROXANNE product. The consortium itself contains some significant professional, gender, cultural, and geographic diversity, which is further extended with by the project Stakeholder Board and global survey respondents. Another key aspect in this regard is ensuring that all analysis of gathered feedback is conducted in an anonymous way in order to uphold the impartiality of the needs assessment. Project partners have been doing this and will continue to do so.

Lawful operation

Thirdly, the potential acquisition and use of the ROXANNE solutions must be compatible with applicable domestic and regional legislation and framed by organisational codes of use and standards. To this end, a well-thought and technically robust design of the ROXANNE platform secured during the project's development stage would enable a transparent and accountable use of the technology adaptable to national provisions. Although the reliance on novel analytical methods often lacks specific guidance, encouraging legislative, policy, and strategy developments are emerging in the area.[61] Furthermore, in the context of the exploitation planning discussion, as well as within meetings of the Ethics Boards, the project team has been considering the implications of the misuse of ROXANNE solutions', including safeguards for a non-discriminatory application of the ROXANNE tools. This could potentially occur should the tool land in the hands of non-democratic regimes or criminal groups that could use it to target vulnerable communities such as refugees or minority groups. Therefore, the consortium is currently in the process of considering commercialisation measures, such as 'know your customer' policies or conducting due diligence assessment, as well as contractual clauses that prohibit the further resale of the ROXANNE platform and enable centralized software control.

Article 47 – Right to an effective remedy and a fair trial

This right is defined as:

> *'Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.*
> *Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.*
>
> *Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.'*

Article 47 of the EU Charter of Fundamental Rights embodies the EU legal principle that Member States must ensure effective judicial protection of an individual's rights arising from Union law (including Charter rights). This means that the right of access to a court applies whenever rights and freedoms guaranteed by EU law are involved. It is for EU Member States to establish a system of legal remedies and procedures that ensure respect for rights under EU law.[62]

Access to court is implicit in the right to a fair hearing because it suggests that disputes must be decided by courts. This right is an important element of access to justice given that courts provide protection against unlawful practices and uphold the rule of law. For the right of access to a court to be effective, states may have to provide legal aid, translation or other practical support to enable individuals to access court proceedings.[63]

Relevance and use to the project

Under this project, this right holds much importance with respect to the need for a 'fair trial'. Whether a hearing is considered fair depends on all facts of the case, including the ability of the individual to access justice. The proceedings as a whole must be considered.[64] One of the core requirements of the right to a fair hearing is 'equality of arms' between the parties. This involves ensuring that each party has a reasonable opportunity to present its case in conditions that do not disadvantage either party.

In terms of prosecutions using evidence analysed through the ROXANNE platform, it may so happen that due to lack of complete algorithmic transparency, the results of this platform could not be completely explained or understood by the accused and/or the prosecutor. In such a case, the weighting given to the results of this platform could play a major role in ascertaining whether the trial is fair or not. Also, it might be difficult to share the evidence with the accused if the internal

analysis and algorithms form a major component of the result which is deemed evidence against the accused. This could further undermine the 'equality of arms' since the evidence brought forth by an 'opaque' platform cannot be disproven without understanding the internal functioning of it, which itself creates a major disadvantage for the defendant.

Hence there is a need to ensure a level of algorithmic transparency which is just enough to verify the results of the platform. Further, the court should be well informed about the possible biases/ technical constraints which might lead to an incorrect result. The confidence level of the result and understanding of the platform should then empower the court enough to make a fair trial. Then, ensuring fair trial would be a function of competency of the court.

Article 48 – Presumption of innocence and right of defence

This right is defined as:

> *'1. Everyone who has been charged shall be presumed innocent until proved guilty according to law.*
>
> *2. Respect for the rights of the defence of anyone who has been charged shall be guaranteed.'*

This Article is the same as Article 6(2) and (3) of the ECHR. In accordance with Article 52(3), this right has the same meaning and scope as the right guaranteed by the ECHR. This article promises that an individual shall be presumed innocent until proven otherwise.[65]

Relevance and use to the project

The ROXANNE platform (when in use) uses network analysis to highlight individuals in a dataset who might have interacted with a 'suspect'. In such a scenario, the individual who otherwise should be presumed innocent, is being monitored. Similarly, ROXANNE might highlight someone innocent who might be a close acquaintance of known suspect(s). Such scenarios need to be dealt with carefully and the onus of the same falls on the end-users and courts. It becomes imperative to complement the results of ROXANNE with some other convincing evidence gathered during the investigation. Unless there is this additional evidence supporting the suggestions of ROXANNE platform or unless the result of the ROXANNE can be verified, the defendant should be given the benefit of doubt.

Having said that, however, it is important that the ROXANNE partners build the platform so that it is transparent enough that people can understand how it works well enough that this can be explained in a court-room setting for a jury.

3. SCENARIOS

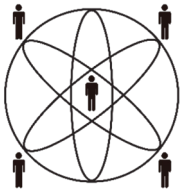
The below scenarios are entirely fictional; they present situations where tools like those in the ROXANNE platform could be used and things go wrong. The intention of doing this is to highlight issues that need to be raised and considered (with the focus here on societal issues). Once issues are highlighted, we can focus on developing solutions so that these incidents do not happen with ROXANNE. We would appreciate any feedback you wish to provide, especially if you could provide answers to the questions that are asked. You will be able to respond to these questions via a link to a survey that is available on the ROXANNE project website.

Scenario 1 – Violent and peaceful protesters

Katy runs a political campaign group that organises protests for better representation of ethnic minorities in public life. She organises a march to support this cause. During the march, a small faction of protesters engages in violence.

In order to identify the violent protesters, LEAs analyse all CCTV of the march using the ROXANNE facial verification tool. This analysis shows that the faction instigated violence at several different sites during the march. The faction is ethnically diverse, but only the violent protesters who are from an ethnic minority are known to the police due to discriminatory policing practices in the past. LEA officers arrest and interview the violent protesters from ethnic minority groups who they have identified.

The ROXANNE consortium should do all that it can to alleviate risks of this happening through evaluating all the data sets which it is using to train the platform on to ensure that they are not biased for or against different groups, and ensuring that the platform is measuring data that is representative. This should, therefore, reduce the risk of the ROXANNE platform having a discriminatory effect when it is used.



Question: In order to protect rights of non-discrimination, how should LEAs prevent bias in historical data and historical policing practices from affecting policing activities today?
Answer:

During interviews, violent protesters acknowledge their membership of Katy's campaign group but those in the violent faction refuse to reveal information about other members of the faction. In order to identify faction members, investigators obtain a warrant to examine the communication data of the violent protesters. Investigators analyse the mobile phone data of the offenders using the ROXANNE platform. The results of this analysis reveal other members of the faction and also show that Katy is connected to every offender. Investigators question the violent protesters about whether Katy had any role in instigating violence and conclude that she was not involved.

Question: If the personal data of an innocent person is included in an investigation, how should LEAs balance respecting rights to privacy and the protection of personal data with the needs of an investigation? What factors should be considered?
Answer:

After being released on bail, several of the violent protesters inform Katy that investigators asked questions about her. Katy worries that LEAs will take an interest in her because she organised the march, this leads to high-levels of stress which badly affect her mental health and she passes the leadership of her campaign group to other people.

Question: In order to balance protecting the integrity of the person with needs to protect the public, should LEAs consider the indirect effects that their actions might have on people, particularly if it results in the suffering of those being investigated? Should indirect effects be judged in terms of the proportionality of LEA actions?
Answer:

Following the identification of other members of the violent faction using ROXANNE, they are also arrests. This, combined with the apparent LEAs' interest in Katy, leads peaceful leaders of the campaign group to mistakenly determine that LEAs are trying to deter further peaceful protests. Based on this belief, peaceful campaigners cancel future protests owing to the perceived risks of arbitrary arrest and protesters believing LEA actions to be an attack on their freedoms of expression and assembly.

Question: In order to respect freedoms of expression and assembly and avoid chilling effects, how should LEAs balance the need to communicate their lawful and ethical use of technology in order to build public trust with the need to keep sensitive investigative information and techniques secret so as not to benefit criminal perpetrators?
Answer:

Please use this box to provide any feedback you might have about the scenario as a whole, or any other comments you might have about the implications of ROXANNE for fundamental rights.

Scenario 2 – Extreme writings

Alex is a literature student who is interested in writing about extremist politics. The plot for one of their stories advocates violence in support of an extreme political cause. Alex's university professor is concerned about this and flags the story to the university who report it to a local LEA.

LEA officers assess all information openly available about Alex on the internet, including their social media pages and blog. The LEA analyses this information using the ROXANNE text analysis tools and discovers many mentions of 'guns' and 'bombs', along with many references to killing political enemies.

Question: In order to protect privacy rights, LEA processing of personal data should be restricted to what is lawful, necessary, and proportionate. But, should there be any additional restrictions on LEAs accessing information about suspects that is openly available (e.g. only processing data where citizens would reasonably expect it)?
Answer:

LEA officers are concerned that Alex might be involved in a plot to commit violence and obtain a warrant to intercept Alex's internet traffic to ascertain if this is true. LEAs discover that Alex has been communicating with many political extremists after evaluating their internet traffic. Using network analysis, they show that Alex links several extreme groups across the political spectrum.

Motivated by their growing concerns about Alex's potential plans, investigators present these initial findings to a judge and obtain a warrant for accessing Alex's content data. They discover a large number of Alex's private writings in an online drive; these are analysed using the ROXANNE text analysis tool which shows that Alex has written a manifesto that includes both violent language and plans for attacking specific targets. LEA officers are convinced that Alex is preparing for an act of terrorism and they arrest Alex.

Question: In order to prevent automated decision-making, and to respect rights to liberty and security, how should LEA officers corroborate the results of data-analysis tools before they arrest someone? For example, an investigator could repeat the machine analysis to ensure it is correct, check that key results make sense, or find additional corroborative evidence before acting.
Answer:

Alex's case reaches the trial stage. The prosecution presents the results of analysis done by the ROXANNE platform to show that Alex has been communicating with political extremists, has written extensively on violent political extremism, and has developed specific plans for carrying out violent acts. The defence case argues that Alex is innocent and was communicating with political extremists for a book project that would include samples from a fictional manifesto that includes fake attack plans.

Question: In order to protect the right to a fair trial, should the use of technological results be subject to review by experts before being submitted to court? Should the results be presented in court by experts, as with forensic evidence?
Answer:

The jury are extremely impressed with the technological sophistication of the ROXANNE platform and give the results from the platform greater weight in their discussions than other evidence. They jury convict Alex, although Alex is actually innocent.

Question: In order to protect the presumption of innocence, should safeguards be implemented so that juries can understand, and give a fair assessment of, the results of technological analysis? If so, what safeguards?
Answer:

Please use this box to provide any feedback you might have about the scenario as a whole, or any other comments you might have about the implications of ROXANNE for fundamental rights.

ROXANNE

REFERENCE

1 This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833635

2 Sabine Michalowski, 'Article 3', in Steve Peers, Tamara Hervey, Jeff Kenner, and Angela Ward (eds.), 'The EU Charter of Fundamental Rights: A Commentary' (Hart Publishing, 2014) (hereafter: Michalowski, 2014), para.03.01.

3 See Jalloh v Germany App no 54810/00 (ECtHR, 1 July 2006)(hereafter: Jalloh, 2006); Dordevic v Croatia App no 41526/10 (ECtHR, 24 July 2012) (hereafter: Dordevic, 2012)

4 Michalowski, 2014, para.03.20; Jalloh, 2006, para.79; Jehovah's Witnesses, 2010, p.135.

5 Jehovah's Witnesses of Moscow v Russia App no 302/03 (ECtHR, 10 June 2010) (hereafter: Jehovah's Witnesses, 2010), p.135; Pretty v UK App no 2346/02 (ECtHR, 29 April 2002) p.63.

6 See, for example, Jalloh 2006,, p79.; Dordevic, 2012, p.95.

7 And physical integrity also, see A, B, and C v Ireland App No 25579/05 (ECtHR, 16 December 2010), p.245.

8 Explanation on Article 6 - Right to liberty and security, CFR Explanations.

9 De Tommaso v Italy App No. 43395/09 (ECtHR, 23 February 2017), para.80.

10 Guzzardi v Italy App No 7367/76 (ECtHR, 6 November 1980), para.95.

11 Daniel Wilsher, 'Article 6', in Steve Peers, Tamara Hervey, Jeff Kenner, and Angela Ward (eds.), 'The EU Charter of Fundamental Rights: A Commentary' (Hart Publishing, 2014)(hereafter: Wilsher, 2014), para.06.14.

12 Lyon, David., The Electronic Eye, University of Minnesota Press, Minneapolis, 1994, p.63.

13 Explanation on Article 7 – Respect for private and family life, CFR Explanations.

14 Jens Vedsted-Hansen, Article 7 (Private Life, Home and Communications), in Steve Peers, Tamara Hervey, Jeff Kenner, and Angela Ward (eds.), 'The EU Charter of Fundamental Rights: A Commentary' (Hart Publishing, 2014)(hereafter: Vedsted-Hansen, 2014), para.07.23A-07.24A, 07.66A-07.73A

15 Vedsted-Hansen, 2014, para.07.21A-.7022A

16 Vedsted-Hansen, 2014, para.07.24A

17 Vedsted-Hansen, 2014, para.07.08A

18 Vedsted-Hanson, 2014, para.07.11-07.20A

19 Shazia Choudhry, Article 7 (Family Life Aspects), in Steve Peers, Tamara Hervey, Jeff Kenner, and Angela Ward (eds.), 'The EU Charter of Fundamental Rights: A Commentary' (Hart Publishing, 2014)(hereafter: Choudhry, 2014), para.07.20B

20 Choudrhy, 2014, para.07.02B-07.04B

21 Choudhry, 2014, para.07.05B-07.06B

22 Choudhry, 2014, para.07.07B-07.09B

23 Dudgeon v The United Kingdom App No 7525/76 (ECtHR, 22 October 1981), para.51.

24 Paradis and Campanelli v Italy App No 25358/12 (ECtHR, 24 January 2017), paras.179-184.

25 Lambert v France App No 23618/94 (ECtHR, 24 August 1998), para.21.

26 Iordachi and Others v Moldova App No 25198/02 (ECtHR, 14 September 2009), para.44.

27 Amann v Switzerland App No 27798/95 (ECtHR, 16 February 2000), para.61.

28 Amann v Switzerland App No 27798/95 (ECtHR, 16 February 2000), para.61.

29 Art.15, GDPR

30 Art.16, GDPR

31 Art.17, GDPR

32 European Union Agency for Fundamental Rights, Handbook on European data protection law, FRA, Luxembourg, 2018, pp.17-18.

33 Z v Finland App no 22009/93 (ECtHR, 25 February 1997)

34 Krone Verlag GmbH v Austria App no 431/96 (ECtHR, 26 February 2002); Von Hannover v Germany App no 59320/00 (ECtHR, 24 June 2004)

35 Leander v Sweden App no 9248/81 (ECtHR, 26 March 1987); Gaskin v UK App no 10454/83 (ECtHR, 7 July 1989), para.49

36 Klass v Germany App no 5029/71 (ECtHR, 6 September 1978)

37 I v Finland App no 20511/03 (ECtHR, 17 July 2008), para.38-40

38 CJEU, Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen [GC], 9 November 2010 (hereafter: Land Hessen, 2010), para. 48.

39 Land Hessen, 2010, para.51

40 See, for example, Article 8, European Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) 213 UNTS 221.

41 On Scientific research being a legitimate objective for data processing, see Recitals 156-158, GDPR.

42 Hasham and Harrup v the United Kingdom App No 25594/94 (ECtHR, 25 November 1999).

43 K v. Austria App No 16002/90 (ECtHR, 13 October 1992), para.45.

44 Case C-316/09 MSD Sharp & Dohme GmbH v Merckle GmbH, CJEU, Opinion of AG Trstenjak 24 November 2010, para.81.

45 Neij and Sunde Kolmisoppi v. Sweden App No 10397/12 (ECtHR, 19 February 2013), dec.

46 Mavlanov and Sa'di v Uzbekistan U.N. Doc. CCPR/C/95/D/1334/2004 (HRComm, 19 March 2009, para.6.1.

47 Sürek v Tukey App no 24735/94 (ECtHR, 8 July 1999), para.36.

48 Maegulev v Russia, App No 15449/09 (ECtHR, 8 January 2020).

49 Navalnyy v. Russia App No 29580/12 (ECtHR, 15 November 2008), para.102; Friend, the Countryside Alliance and others v. the United Kingdom App No 16072/06 and 27809/08 (ECtHR, 24 November 2009), para.50.

50 Emin Huseynov v. Azerbaijan App No 59135/09 (ECtHR, 7 August 2015), para.91.

51 Djavit An v. Turkey App No 20652/92 (ECtHR, 9th July 2003)(hereafter: Djavit An, 2003), para.60.

52 The Gypsy Council and Others v. the United Kingdom App No 66336/01 (ECtHR, 14 May 2001)(dec.).

53 Barankevich v. Russia App No 10519/03 (ECtHR, 26 October 2007), para.15.

54 Kudrevičius and Others v. Lithuania App No 37553/05 (ECtHR, 15 October 2015), para.91;Djavit An, 2003, para.56.

55 Young, James and Webster v. the United Kingdom, App Nos 7601/76 and 7806/77 (ECommHR, 14 December 1979), para.167.

56 McFeeley v. the United Kingdom App No 8317/78 (ECommHR, 15 May 1980), para.114; Bollan v. the United Kingdom App No 42117/98 (ECtHR, 4 May 2000) (dec.).

57 Christian Democratic People's Party v. Moldova App No 28793/02 (ECtHR, 14 May 2006), para.77.

58 Nurettin Aldemir and Others v. Turkey App Nos 32124/02, 32126/02, 32129/02, 32132/02, 32133/02, 32137/02 and 32138/02 (ECtHR, 2 June 2008), para.34; The United Macedonian Organisation Ilinden and Ivanov v. Bulgaria App No (ECtHR, 15 February 2006), para.135.

59 Bączkowski and Others v. Poland App No 1543/06 (ECtHR, 24 September 2007), paras.66-68.

60 « Data-driven policing : the hardwiring of discriminatory policing practices across Europe » Patrick Williams and Eric Kind ENAR, November 2019, https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf
AI expert calls for end to UK use of 'racially biased' algorithms', The Guardian, 12 December 2019, https://www.theguardian.com/technology/2019/dec/12/ai-end-uk-use-racially-biased-algorithms-noel-sharkey

61 New Zealand claims world first in setting standards for government use of algorithms, The Guardian, 27 July 2020, https://www.theguardian.com/world/2020/jul/28/new-zealand-claims-world-first-in-setting-standards-for-government-use-of-algorithms ; The ethics of artificial intelligence: Issues and initiatives, European Parliament, Study, March 2020, pp. 66-84 https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf; Jobin, A., Ienca, M. & Vayena, E. The global landscape of AI ethics guidelines. Nature Machine Intelligence 1, 389–399 (2019). https://doi.org/10.1038/s42256-019-0088-2

62 CJEU, C-432/05, Unibet (London) Ltd and Unibet (International) Ltd v. Justitiekanslern, 13 March 2007, paras. 37–42.

63 European Union Agency for Fundamental Rights and Council of Europe, "Handbook on European law relating to access to justice",European Union Agency for Fundamental Rights and Council of Europe, 2016,

p.26. Available at: https://www.echr.coe.int/Documents/Handbook_access_justice_ENG.pdf

64 Edwards v. the United Kingdom, App No 13071/87 (ECtHR,16 December 1992), para 34

65 Art.6(2), ECHR