Fostering Transparency of Judicial Decisions and Enhancing the National Implementation of the ECHR (TJENI)

Workshop on anonymisation (pseudonymisation) of judicial decisions
Report

Paris

29 November 2022

The opinions expressed in this work are the responsibility of the authors and do not necessarily reflect the official policy of the Council of Europe.

The project "Foster Transparency of Judicial Decisions and Enhancing the National Implementation of the ECHR" (TJENI) is funded by Iceland, Liechtenstein and Norway through the EEA and Norway Grants Fund for Regional Cooperation

Table of Content

Introduction

The TJENI Project, including 6 participating countries (Cyprus, Hungary, Lithuania, Poland, Romania and Slovenia) and funded by Iceland, Liechtenstein and Norway through the EEA and Norway Grants Fund for Regional Cooperation, aims to propose methodological and technological solutions for anonymisation (pseudonymisation) of judgments for their online publication and categorisation.[1]

Against this background, on 29 November 2022, a workshop on the anonymisation (pseudonymisation) of judicial decisions took place in the Council of Europe office in Paris. Introduced by Tigran Karapetyan, Head of Division of Transversal Challenges and Multilateral Projects, DG I, and concluded by Frédéric Dolt, Head of Department of Implementation of Human Rights, Justice and Legal Co-operation Standards, DG I, the workshop hosted 47 (22 online) participants and thirteen experts sharing their knowledge and exchanged on such questions as regulatory framework requirements and safeguards and remedies for human rights protection, technical tools and applications in use, Machine Learning (ML) and Natural language processing (NLP), interoperability and cybersecurity .

Total *number of participants (in person and online) – 47*
In person *participants – 25 (11 F, 14 M)*
Online *participants – 22*
Gender *count (in person and online) – 19 F, 28 M*

Opening remarks

Tigran Karapetyan opened the event and pointed out key areas for further discussions like privacy, anonymity, usability, security, and re-identification of personal data related to the subject of anonymisation of court decisions. He stressed that the goals of publication of judicial decisions should be determined by the partners in order to secure balancing of human rights (such as the right to personal data protection and the right to access judicial decisions) and open data and access to information. He also pointed out the right to be forgotten and to rehabilitation demanded as important aspects for consideration of the length of open access to judicial decisions. Risks of re-identification were highlighted in light of a necessity to have a regularly updated methodology to assess specific risks in response to the constant development of different technologies. One element of the TJENI project focuses on the development of specific safeguards and legal remedies. The second component of the project addresses the consistency of national jurisprudence with a focus on the categorisation of case law, its organisation within the national systems and its connection to the European Court of Human Rights case law and knowledge sharing databases. Based on the findings of the initial needs assessments, the development of action plans was initiated for each of the TJENI partner countries including recommendations on the regulatory framework, policies and anonymisation methodologies. Moreover, special attention in the individual action plans should be paid to the organisation and the interoperability of databases, the use of automated tools as well as the related risks and addressing partner countries' training needs After the workshop, the action plans will be discussed and finalised with each TJENI project partners followed by its implementation in 2023 until the end of the project.

[1] *Council of Europe*, Foster Transparency of Judicial Decisions and Enhancing the National Implementation of the ECHR (TJENI); https://www.coe.int/en/web/national-implementation/tjeni [28/11/2022].

Regulatory framework requirements

Elena Yurkina, Head of Unit, Innovative Solutions for Human Rights and Justice, DG I, presented a compilation prepared under the project on various questions related to on-line publication of judicial decisions. The compilation represents a collection of various recommendations and documents of CoE bodies (such as CM, CCJE, CEPEJ and other CoE Commissions and Committees). It also contains description of relevant case law of the ECtHR.

The purpose of this document is to bring together different recommendations and provide the project partners with an overview of the questions that shall be consider in connection with on-line publication of judicial decisions. Special considerations were also given to human rights protection. The document includes a checklist to support such considerations.

Going deeper into the content of the compilation, Ms Yurkina, presented that an underlying regulatory framework is essential in case of interference in the privacy (the rights set in Article 8 of the ECHR). In case of a case brough to the ECtHR its examination from the point of view of the ECHR could primarily focus on the assessment of the legal framework and the provision of procedural remedies.

Speaking in more details about the goals and objectives of online publication of judicial decisions, she referred to the Committee of Ministers Recommendation Rec (1995) 11 concerning the Selection, Processing, Presentation and Archiving of Court Decisions in Legal Information Retrieval Systems, the CM Recommendation Rec (2001) 3 on the delivery of court and other legal services to the citizen through the use of new technologies and other documents mentioned in the compilation. Also, in terms of processing, anonymisation itself, case law databases, the scope of publication, interoperability, Artificial Intelligence, big data, and archiving there were several Committee of Ministers Recommendations which the member states could rely on. The setup of the further development of an ICT environment requires consideration of human rights protection, in particular, the privacy of individuals, the judicial independence, user friendliness as well as a regular project evaluation and assessment during all stages. Finally, the training of the users is an important element in such process, both technological aspects (handling of the tools) and legal (risks related to personal data).

Safeguards and remedies linked to anonymisation (pseudonymisation)

Silvia Martinez Canton, Council of Europe expert and seconded judge at the CJEU, reported about the Spanish system and its approach to anonymisation of court decisions, implemented safeguards and legal remedies. The respective Spanish legal framework, amended in 2001, distinguishes between processing of personal data carried out for judicial and non-judicial purposes. Judicial data is related to judicial proceedings and thus considered to being processed for judicial purposes. This distinction triggered different competencies, on the one hand, that of the General Council of the Judiciary, on the other hand, that of the Spanish Data Protection Agency. This system guaranteed the independence of the judiciary from the governmental branch. The General Council of the Judiciary acted as a monitoring body by means of inspections, guidelines, or reports on the proper application of data protection regulations, information on request on any data subject and its data protection rights and processing of individual complaints. While in absence of an explicit regulation each court itself serves as a controlling authority in terms of data protection. The Judicial Documentation Centre (CENDOJ) under the General Council of the Judiciary is responsible for the centralised publication of court decisions in Spain (except those by the Constitutional Court which is under a separate regime based on a ruling of the Constitutional Court of 23 July 2015) and their anonymisation conducted by a private company awarded with a public contract. CENDOJ provided access to the database of judicial decisions, which was open and free of charge. While in Spain almost all Supreme Court decisions were published, judgments of lower instance courts are selected for publication on the basis of their legal interest. The private company designed a tool combining fully automated processing and jurisprudential referencing with human administered checks in terms of anonymisation and additional proofreading of sensitive cases. The Spanish tool used fictional pseudonyms to replace first and last names of individuals involved in the proceedings and all data allowing for conclusions being drawn. At the same time officials like judges, magistrates or legal representatives are not anonymised as well as companies not consisting of real persons' names. There were some exceptions to this general rule when it comes to tax fraud cases. For the preliminary ruling regime of the European Court of Justice, the Spanish courts did not consult CENDOJ but relied on a recommendation of 2018 causing, in some cases, different versions of the same judgment. In case of an infringement of the right to privacy, individuals were allowed to lodge complaints with the Data Protection Agency (regarding non-judicial data), or the General Council of the Judiciary (in terms of judiciary related data). When the Data Protection Agency has no competency to deal with a complaint it forwards such complaint to the General Council of the Judiciary. In case of failures in the course of the anonymisation process, an ex-officio investigation could be launched by the director of supervision and control of data protection or the data protection committee at the General Council of the Judiciary with a concrete impact on the processing and organisation of the administration of justice. Another way to obtain justice were state liability procedures, initiated ex officio or by means of an individual claim. Additionally, private responsibility under criminal or civil law is an additional option. Spain amended the data protection system according to several cases before the ECtHR (Del Campo vs. Spain) and the ECJ (Google vs. Spain). Finally, Ms Martinez also addressed the most pertinent cases and practice of the Court of Justice of the European Union with regards to the publication of their decisions.

Overview of some technologies and advanced tools for anonymisation of judicial decisions

Gernot Posch, Council of Europe Expert, provided an overview of advanced tools for anonymisation of court decisions in some Council of Europe member states based on a survey conducted in 2022, interviews with stakeholders and online research. The results allowed to compare and demonstrate the tools used in Austria, Denmark, Finland, Italy, Latvia, and Switzerland. As regards private solutions, there are not that many specialised private companies concentrating on tailored solutions for the anonymisation of judicial decisions and meeting, at the same time, the high expectations of the judiciary. On the other hand, lacking the special know-how when it comes to the design and implementation of such advanced tools, public stakeholders seemed to prefer cooperation with private providers. Starting from a five-point analysis pattern (principles, user surface, workflow, architecture, and results), the solutions identified in the listed countries were analysed and rated. While all models had in common that they strived for a result of high quality and to minimise the efforts in terms of time and staffing, the approaches are quite different. Some of the countries favour more automated solutions simply providing automated processing of the anonymisation without any options being adapted by the users resulting in a clearly divided workflow (post-processing). Others relied on a semi-automated approach, meaning that the human administered quality check already intervened in the stage of anonymisation (pre-processing). The latter provided the user different editing functions saving time but requiring better trained staff. Some of the solutions are fully integrated in the court environment and respectively the Court Case Management Systems (CCMS) as well as the publication workflow. Some provide for separate anonymisation working independently. Most of the systems relied, technically speaking, on the method of Named Entity Recognition (NER), a category of Natural Language Processing (NLP). The fully integrated models have the advantage of drawing reliable data from the CCMS, which helps the systems improve precision. Cloud-based solutions appeared to be more the exception than the rule. The results achieved by automated solutions seemed to be promising though none of the systems worked without human intervention. Some solutions enabled multi-format support (Pdf, word, html, odt.), others even provided multilingual versions.

Demonstration of some tools

Martin Schneider, Council of Europe consultant, presented the Austrian tool for anonymisation embedded in the technical environment of the Court Case Management of the Austrian Judiciary. Although the Austrian legal framework only provided for an obligatory publication of Supreme Court decisions while lower instance court decisions remained unpublished, the principles of transparency and open justice demanded for a broader interpretation, as laid down in the governmental agenda 2020-2024. The solution was the development of an Artificial Intelligence based automated application, which facilitated to anonymise all decisions in the internal database and to publish a higher number than before in the Austrian Legal Information System. Despite it was a far advanced automated solution, the publication on the public platform still required human-administered quality checks and manual editing when necessary. The tool comprised different Machine Learning (NLP) and rule and dictionary-based services. The system had been trained on a sample of 66.000 decisions of the Supreme Court, 800.000 decisions of other courts, and publicly available data.

Natural and legal persons as well as locations or other information of were replaced by a letter/star-pattern (A*, B*) if occurring more than once in a text, otherwise only by a two-star pattern (**) without letters. The names of judges and legal representatives remained unmasked. The key performance indicators of the tool (recall, precision and F1 score) had improved a lot in recent years and recently found themselves around 93% on average (only some points below human administered anonymisation). The anonymisation tool provides an annotated and a final version of the judgment. The application provides to the user some options for categorisation and tagging of decisions and asks for internal or external publication.

Sylvie Postel, Auditor in charge of the Digital Law and Data Protection Office, SDER, French Court of Cassation, pointed out that the French practice of publication of court decisions is based on a law of 2016 (amended in 2019 and 2020) providing access to open judicial data. Based on that, the Court of Cassation made available online all decisions of the French jurisdiction free of charge. Pseudonymisation was crucial to guarantee the integrity of the judicial decisions that are publicly available. Although the French anonymisation approach was holistic, including the names of natural persons, parties and third parties, the names of the judges, clerks or legal representatives remained non-pseudonymised. The automated anonymisation also comprises legal persons, addresses and locations, identifiers like telephone or fax numbers, national identity numbers, banking details, emails, and registration plates though on a voluntary basis. It would be up to the judge whether to mask complementary elements endangering the privacy or physical integrity of a person. The National Freedom Commission recently published several guidelines on the question how to harmonise additional anonymisation acts instructed by judges. At the Court of Cassation, the president of the chamber is responsible to tick which categories are being anonymised. The anonymisation practice had been rolled out at first instance courts lately, criminal court decisions were on the 2024 agenda.

Amoury Fouret, data scientist at the French Court of Cassation, presented the inhouse solution implemented in 2019 after having quit the contract with an external service provider. From then on, the number of court decisions being published scaled up from 10,000 to 300,000 per year. The future goal is to have 3 million decisions published annually.

The French application based on deep learning engines and including an ergonomic annotation interface, had been trained on 2 million rulings of the Court of Cassation and the Courts of appeal and edited versions of human editors. The tool not only involved a model for legal language but also a powerful calculation tool identifying different categories confirmed by a human. Better the machine-based detection works, less personnel is needed. According to Amoury Fouret the new tools halved the correction time. The dynamic data approach requires to track the evolutions being made by dint of data version control (DVC). For testing, the Court of Cassation followed a unit testing approach which guaranteed detecting instantly the mistakes made by the machine and improving performance in the future. The post processing by a human checker by means of the annotation interface is of major importance to train the machines to reach the future goal of 3 million decisions a year. The annotation interface is an open-source system with different features designed to allow a large group of people editing at the same time. For the administrator, the system shows some statistics, for example the number of documents having been processed. The system had been improved over the last few years, so that some decisions no longer require proofreading at all or only partly. Important decisions are still checked or double checked by the editor or his/her supervisor respectively. The previous pseudonymisation pattern (brackets with three points in between) had been replaced by a more comprehensible model (names by letters in braces, other entities with the category and a number in braces).

Machine learning and natural language processing

Murielle Popa-Fabre, Council of Europe expert, illustrated the latest results in NLP related sciences. Artificial Intelligence is the product of having a good code, efficient computing power and data of good quality. While the first two had been the challenges of recent years, a data centred approach to AI is in the middle of interest these days. One of the most impressive algorithms, the Bloom mega language model, only having been published this summer, could also be of importance for the anonymisation of court decisions. The model involving 1000 researchers included 59 languages, had been trained on 1,5 TB of data and consisted of 176 billion parameters. 5 million hours of calculation based on the power of 3,500 GPUs were invested in the project. The design of the project also allowed the inclusion of rarely used language families. Despite its huge scope of application, the model was not that useful when it comes to its application in a very specific field, like legal language since the accuracy of the tool shall be very high. Hence, the models tended to go domain specific, like JuriBERT, which had been trained on the information crawled from a French legal website provided by the government and including court decisions. The model reached quite good results in classification of pleadings. One disadvantage of these NLP models is their static design requiring a lot of work keeping it up to date using retrieval models functioning on the creation of structured relationships. Another important aspect that needs to be taken into consideration is biased dataset used for the development of the NLP model. This requires implementing strategies to measure bias in NLP models in order to minimise and eliminate bias. Balancing between the goals of maximum transparency and a perfectly comprehensible decision and the protection of personal data, the increasing possibilities of re-identification of masked personal data by crossing information and indirect identifiers would be one of the major challenges. Unsupervised de-identification could be one of the approaches to deal with this issue by masking the minimum of terms while achieving better results than by traditional NER methods.

Cosmin Sterea-Grossu, Judge, Head of IT and judicial statistics, Superior Council of Magistracy, Romania, shortly demonstrated the Romanian mechanisms of anonymisation (regular expression, dictionary and metadata based) finding themselves in a transition phase in order to achieve better results relying on more advanced technologies. One of the challenges was the holistic approach not only dealing with final decisions and therefore causing a workload of 3 million documents per year being processed and published in a centralised database. Not only the real-time replication of decentralised stored documents in a centralised node but also the provision of a fast and scalable search engine is one of the major tasks being faced.

Vasile Pais, Senior Researcher, Romanian Academy Research Institute for Artificial Intelligence "Mihai Drăgănescu" (RACAI), introduced the RELATE platform for Romanian language technologies and resources including technologies developed both at the RACAI and by partners in multiple national and international projects. For example, Corolla was one of the flagship projects containing the representative corpus of contemporary Romanian language. The platform itself followed the European language grid philosophy having made use of web services and rest APIs as well as different modules available as containers. RELATE united a publicly available web front end granting demo access to most of the internal functionality. The backend was mainly intended for large corpora and offered features like task scheduling, format converters and storage. It included basic language and notation functionality, like segmentation at different levels, lemmatisation, part-of-speech tagging and dependency parsing. Besides legal domain named entity recognition (IATE, EUROVOC) the platform also provides for Romanian Wordnet terminology annotation, speech recognition and synthesis. The Romanian anonymisation component is based on the Romanian sub-corpus in the framework of the MARCELL project and relies on named entity recognition but also tries to anonymise and replace unknown entities by random pseudonyms of the same quality. For example, locations are replaced by locations, Romanian names by Romanian names, foreign names by foreign names.

Interoperability

Marko Sever, Council of Europe expert, opened the panel on interoperability and defined interoperability as seamless sharing of data. While integration is the sharing information at a certain point of time, interoperability focused on a real-time data connection. A major problem is that most of the digital ecosystems were not designed to communicate with other systems but solely followed their original purpose. Interoperability is a crucial part since communication and data sharing secured predominating influence in ecosystems. It also reflects the ability to access data, to relocate the resources, keep the data secure, and ensure data quality. It is necessary to understand interoperability in a broader sense in order to predefine how systems could be connected to share information efficiently. The biggest challenges are not of technical nature but in the determination of the goals to be achieved in the beginning to prevent cost-intensive adaptations at later stages of the respective projects. From a technical point of view, the implementation in an existing environment and the connection with legacy systems are key factors to implement a properly working anonymisation tool. These principles not only apply to systems on a national level but also with regard to the digital environments of international players. Testing the interoperability part, Marko Sever recommended a four-step action plan (plan, do, check, act).

Tomasz Kisielewicz, Expert in the Modern Technologies Team of the Ministry of Justice, Poland, gave an insight in the functioning of the Polish database offering anonymised judgments of courts in all judicial districts. According to Tomasz Kisielewicz interoperability occurs in different forms and is not only to be reduced to a technological understanding. For example, interoperability also comprises interactions between different courts according to their size and function and the persons responsible. Another form of interoperability takes place between the different stakeholders, be they public institutions or be they private providers, which are responsible for the development of the technical solutions. Interactions between the judiciary and the final user also needs to be considered to ensure user-friendly applications and acceptance. The exchange on existing systems and applications would be helpful for the engineers designing new tools or features. Further crucial elements for an optimum use case design are training of the users, testing and evaluation of the system implemented to ensure transparency and quality of the decisions.

Cyber security

Edouard Rottier, Director of the Open data project, Head of the Case Law Dissemination and Open Data Unit, SDER, Court of Cassation, France, addressed the challenges in terms of cybersecurity from a magistrate's point of view. To guarantee the publicity of judicial decisions, promote a transparency of justice, reinforce confidence in justice, and enhance legal certainty, related security risks have to be accepted and dealt with. France had chosen an open data approach by means of an online accessible database free of charge. To face the problem of profiling of judges' behaviour, criminal responsibility was introduced in the French legal system. The same applies to the re-identification of personal data. There are two major security risks: cyberattacks against the IT system and unlawful use of the open data provided on the internet. Thus, the availability and the efficiency of the system, and the risk relating to the protection of privacy and the protection of private data are at stake. The French Court of Cassation has developed a concrete risk mitigation plan comprising, inter alia, cybersecurity operation and supervision, vulnerability, management access and right management. The concrete measures having been taken were pen tests, upgrading documentation maintenance, maintenance of alerts, monitoring of system vulnerability, security measures for managing accesses and rights as well as training and awareness building for the staff which was a big factor in cybersecurity. A more general risk is the possible interference with the judicial independence and the proper functioning of the justice system. Thus, a regular reassessment of potential risks is important to be able to react immediately.

Florian Blaschegg, Council of Europe expert, tackled the subject of cybersecurity from a technical point of view and outlined the cybersecurity strategy of the Austrian judiciary based on a modern efficient security organisation ensuring an active and flexible response to threats. The security operation centre monitors the security landscape by means of endpoint detection response (EDR), network detection response (NDR), security information and event management. One challenge in this area was to find well educated and skilled personnel, hence, hybrid setups in cooperation with external companies could be a solution. Special security response teams take lead in case of attacks. SIEM is a tool used for forensics to find out the origin of an attack and to improve the processes. The Mitre Attack tool simulated real world scenarios and countermeasures to be taken. The basis of the security landscape is the Endpoint Protection Platform detecting malicious software on devices as well as attacks over the network. It uses signatures, heuristics, firewalls as well as ML technologies to detect possible attacks. Additionally, vulnerability scanners filter the network to detect application servers or open ports matching the information identified with vulnerability databases. Secure software development and zero trust policies are able to reduce the cybersecurity related risks since the possibility of already being hacked has to be taken into account constantly.

Questions and answers sessions

The expert's speeches not only initiated lively discussions of the participating experts and professionals but also tackled the following subject matters:

- Deviating data protection regimes of constitutional courts
- The pros and cons in terms of inhouse, private solutions or mixed solutions
- The importance of a regularly updated framework and methodology
- The efforts in keeping the formatting of judicial decisions
- The contribution of judges in the anonymisation process
- The responsibility and liability of judges in the anonymisation process
- Metrics and statistics to assess the quality of the anonymisation process
- The different scope of publishing judicial decisions (holistic vs. restricted approach)
- The increasing problem of re-identification of personal data
- Efficiency and accuracy of automated tools compared to human administered anonymisation
- The risks related to the replacement of entities with randomly selected real names or terms and biased or discriminating anonymisation
- The risks related to re-identification and cross-linking of information
- The importance of data of good quality and their proper usage
- The advantages and disadvantages of open-source applications
- The origin and frequency of cybersecurity attacks
- The inclusion of human related risks in cybersecurity and the need of awareness raising and training of the users

Conclusions

Frédéric Dolt drew conclusions of the workshop and highlighted the value of the lively discussions on the regulatory framework, the technological aspects of anonymisation and the advanced tools in use for anonymisation of court decisions. Furthermore, the debate had addressed interoperability, cybersecurity, and fundamental aspects in the search for a balance between the benefits and risks of the use of these technologies, like bias, discrimination, or re-identifications of personal data. It is essential to keep in mind that the intent of the TJENI program is to foster transparency of judicial decisions due to technical solutions and to enhance the national implementation of the Convention within the respective member states. The actions of the project will fundamentally contribute to a better understanding of everyone's rights and obligations and to the harmonisation of case law, especially regarding new questions and challenges. Moreover, the TJENI project is particularly innovative, as all participating member states are searching for best practices in terms of anonymising and publishing judicial decisions based on human rights standards and the requirements of the Convention. This approach is reflecting the principle of subsidiarity as laid down in Protocol No. 16 amending the preamble of the Convention and strengthening the principle of subsidiarity. A good implementation of the Convention at the national level, notably through cooperation projects like TJENI, had always been the essential goal of the Council of Europe and had lately been pointed out by the Committee of Ministers. Finally, under the Convention, member states have a broad margin of discretion as to whether and how they published judicial decisions. If publication took place, it is required to be done in line with standards of the Convention. Therefore, the Council of Europe provides the member states continuous support in achieving these important objectives.

Agenda

09.15 – 09.30	**Registration of participants**
09.30 – 09.40	**Opening remarks** • **Tigran Karapetyan**, Head of Division, Transversal Challenges and Multilateral Projects, Directorate General Human Rights and Rule of Law (DGI), Council of Europe
	Regulatory framework for anonymisation (pseudonymisation)
09.40 – 11.00	***Moderator:*** *Elena Yurkina, Head of Unit, Innovative Solutions for Human Rights and Justice, DGI, Council of Europe* **I. Regulatory framework requirements (20 min)** • Overview of CoE recommendations, Elena Yurkina, Head of Unit **Q&A (20 min)** **II. Safeguards and remedies linked to anonymisation (pseudonymisation) (20 min)** • Implementation of recommendations, Silvia Martinez Canton, CoE expert **Q&A (20 min)**
11.00 - 11.15	***Coffee break***
	Tools for anonymisation (pseudonymisation)
11.15 – 12.55	***Moderator:*** *Biljana Nikolic, Senior Project Officer, Innovative Solutions for Human Rights and Justice, DGI, Council of Europe* **III. Overview of some technologies and advanced tools for anonymisation of judicial decisions (30 min)** • Gernot Posch, CoE expert **Q&A (20 min)** **Demonstration of some tools (30 min)** • Martin Schneider, CoE expert • Sylvie Postel, Auditor, Documentation, Studies and Report Department - Head of the Digital Law and Data Protection Office, Cour de cassation / Amaury Fouret, data scientist, Cour de cassation, France **Q&A (20 min)**
12.55 – 14.30	***Lunch break***

14.30 – 15.20

<u>IV. Machine learning and natural language processing (30 min)</u>

- Murielle Popa-Fabre, COE expert
- Cosmin Sterea-Grossu, Judge, Head of IT and judicial statistics, Superior Council of Magistracy, Romania / Vasile Pais, Senior Researcher, Romanian Academy Research Institute for Artificial Intelligence “Mihai Drăgănescu” (RACAI)

Q&A (20 min)

Technological aspects of anonymisation (pseudonymisation): interoperability and security

Moderator: *Laetitia Dimanche, Project Officer, Innovative Solutions for Human Rights and Justice, DGI, Council of Europe*

15.20 – 15.50

<u>V. Interoperatibilty (30 min)</u>

- Marko Sever, CoE expert
- Tomasz Kisielewicz, Ph.D., Expert in the Modern Technologies Team of the Ministry of Justice, Poland

Q&A (20 min)

15.50 – 16.00 ***Coffee break***

16.00 – 16.50

<u>VI. Cyber security (30min)</u>

- Florian Blaschegg, CoE expert
- Edouard Rottier, Auditor, Documentation, Studies and Report Department - Head of digital dissemination office, Cour de cassation, France

Q&A (20 min)

16.50 – 17.00 Concluding remarks

- **Frédéric Dolt**, Head of Department, Implementation of Human Rights, Justice and Legal Co-operation Standards, Directorate General Human Rights and Rule of Law (DGI), Council of Europe