



Anonymization, pseudonymization in eJustice: balancing Open Access and Privacy

Monica Palmirani

CIRSFID-AI,

Research Institute for Human-Centered
Artificial Intelligence, Università di Bologna

26 March 2021



Outline

- Open access and open data for Justice
- Anonymization/ Pseudonymization
- Role of AI
- LegalXML Standards for Explicability
- Conclusions

Open access and open data for Justice



- **Open access and open data**

- Constitutional principle of publicity
- Rule of Law
- Public interest
- Transparency/Effectiveness/Monitoring
- Legal knowledge access (e.g., practitioners, researchers)
- AI new applications

- **Barriers:**

- Political commitment
- Digital transformation
- **Privacy issues**
- Market of private publisher
- **Technical state of the art**



Facebook Twitter
Open Knowledge homepage Blog All posts Donate About us Q

Open Data as a Human Right: the Case of Case-Law

Home / Open Data / Open Data as a Human Right: the Case of Case-Law

July 27, 2016, by [Antoine Dusséaux](#)

14th December 2020

About OGP and Justice

The Open Government Partnership (OGP) provides an opportunity for government and civil society reformers to make government more transparent, participatory, inclusive, and accountable. Working together, government and civil society co-create two-year action plans with concrete commitments across a broad range of issues. All commitments are then monitored by OGP's [Independent Reporting Mechanism \(IRM\)](#). Recently, thanks to increased global activity around justice, many governments and civil society leaders are expressing growing interest in better linking justice with open government.

In this report:

- > [About OGP and Justice](#)
- > [Introduction](#)
- > [Courts](#)
- > [Open Court Data \(pdf\)](#)
- > [Judicial Officers](#)

EN

Official Journal of the European Union

DECISION OF THE COURT OF JUSTICE

of 1 October 2019

establishing an internal supervision mechanism regarding the processing of personal data by the Court of Justice when a

(2019/C 383/02)

Necessity and proportionality

- «Article 5(1) of **modernised Convention 108** which provides: “Data processing shall be **proportionate** in relation to the legitimate purpose pursued and reflect at all stages of the processing a **fair balance** between all interests concerned, whether public or private, and the rights and freedoms at stake” »



EDPS Guidelines on
assessing the
proportionality of
measures that limit the
fundamental rights to
privacy and to the
protection of personal data





Personal data – Art. 4 GDPR

«(1) ‘personal data’ means any information relating to an **identified or identifiable natural person** (‘data subject’); an identifiable natural person is 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; »

Art. 17 Right to erasure (‘right to be forgotten’)



Article 2, paragraph 2 Regulation EU 2018/1807

«2. In the case of a data set composed of both personal and **non-personal data**, this Regulation applies to the non-personal data part of the data set. Where personal and non-personal data in a data set are inextricably linked, this Regulation shall not prejudice the application of Regulation (EU) 2016/679.»

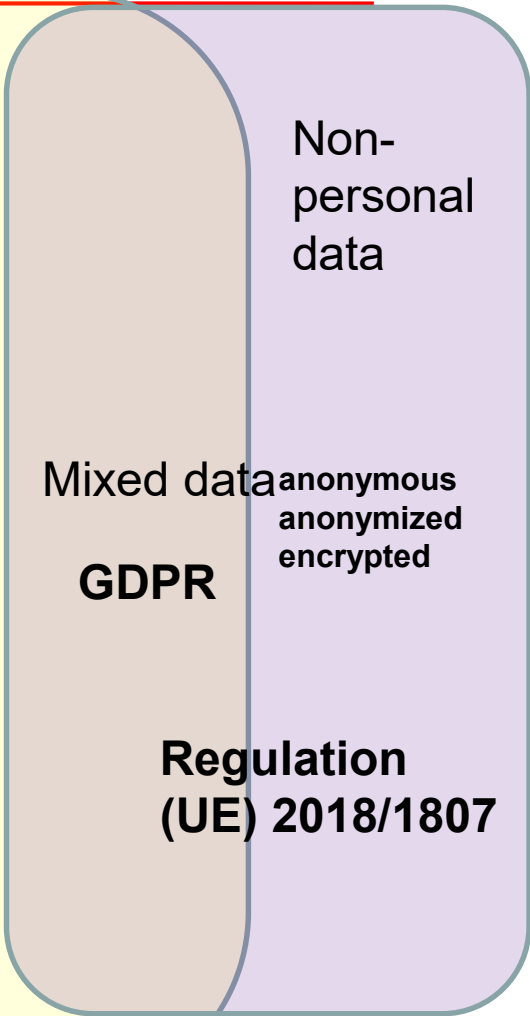


Type of Data

Personal data

GDPR

Pseudo anonymous



Non-personal data

Mixed data
anonymous
anonymized
encrypted

GDPR

Regulation
(UE) 2018/1807



COMMISSIONE
EUROPEA

Bruxelles, 29.5.2019
COM(2019) 250 final

**COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL
CONSIGLIO**

**Guidance on the Regulation on a framework for the free flow of non-personal data in
the European Union**

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0250&from=EN>



Inextricably linked

- «The concept of ‘inextricably linked’ is not defined by either of the two Regulations³⁰. For practical purposes, it can refer to a situation whereby a dataset contains personal data as well as non-personal data and separating the two would either be impossible or considered by the controller to be economically inefficient or not technically feasible.»

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0250&from=EN>

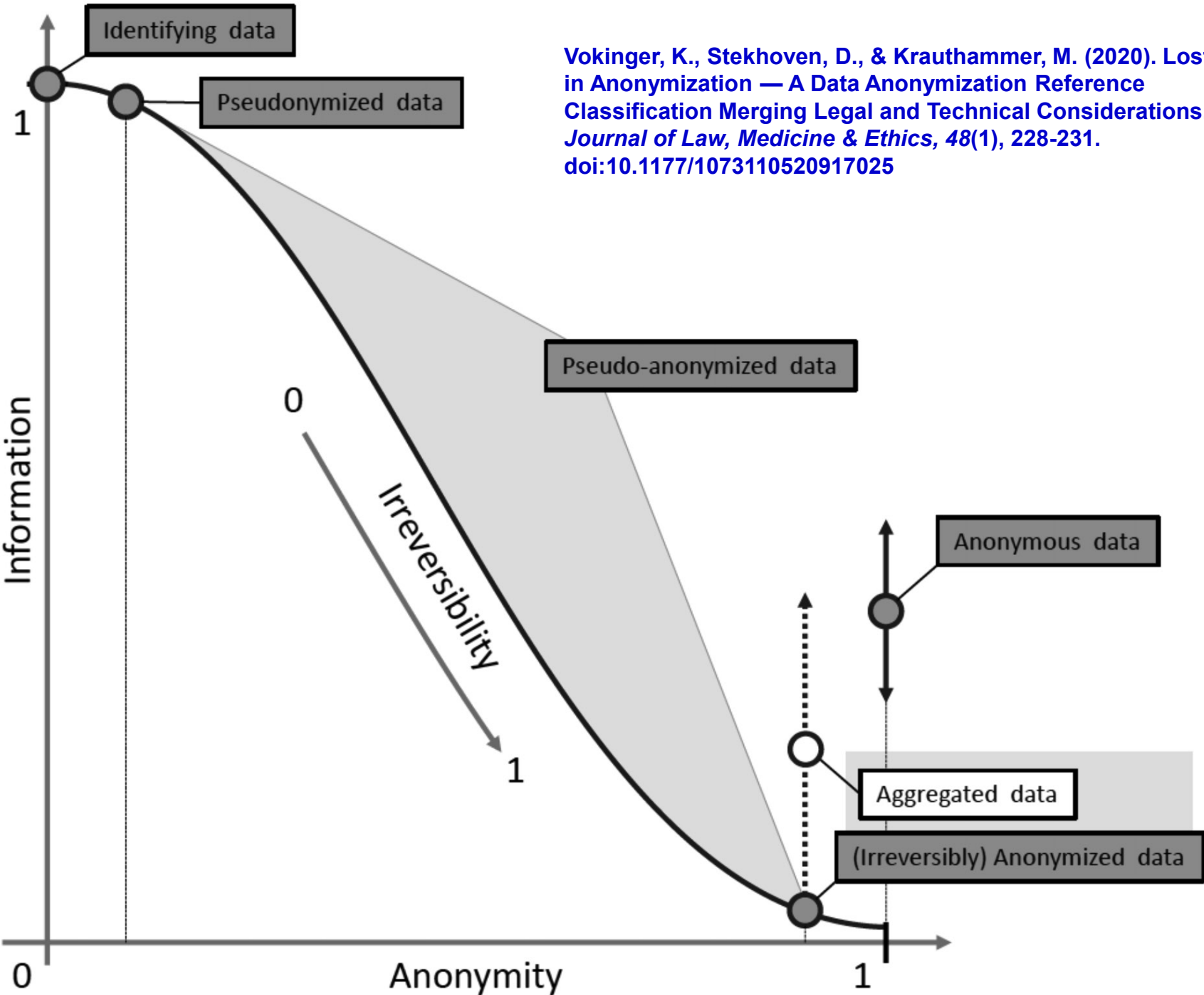


Not affect the legal knowledge

RITENUTO IN FATTO

1. Con sentenza del 18.9.2008, il Giudice per le indagini preliminari del Tribunale di Milano, all'esito di giudizio abbreviato, escluso il concorso con **D.A.** che veniva assolta per non aver commesso il fatto, dichiarava **D.C.** responsabile dei reati ascrittile e di cui agli artt. 40 cpv, 110 609 bis, 609 ter, 572 cod. pen. per non aver impedito il delitto di violenza sessuale e di maltrattamenti in **OMISSIS** commessi da **S.M.** **OMISSIS** della **D.**, in danno **OMISSIS** **S.F.** (capi D ed E) ed il delitto di maltrattamenti **OMISSIS** commesso in danno **OMISSIS** **L.** **N.** e **L.** da **S.M.**, **OMISSIS** e **OMISSIS** della **D.** (capo F) e, concesse le circostanze attenuanti generiche, ritenuta la continuazione fra i reati ed applicata la diminuzione per il rito, la condannava alla pena di anni tre e mesi otto di reclusione ed alle pene accessorie conseguenti, oltre al risarcimento dei danni in favore delle parti civili costituite.

Vokinger, K., Stekhoven, D., & Krauthammer, M. (2020). Lost in Anonymization — A Data Anonymization Reference Classification Merging Legal and Technical Considerations. *Journal of Law, Medicine & Ethics*, 48(1), 228-231. doi:10.1177/1073110520917025

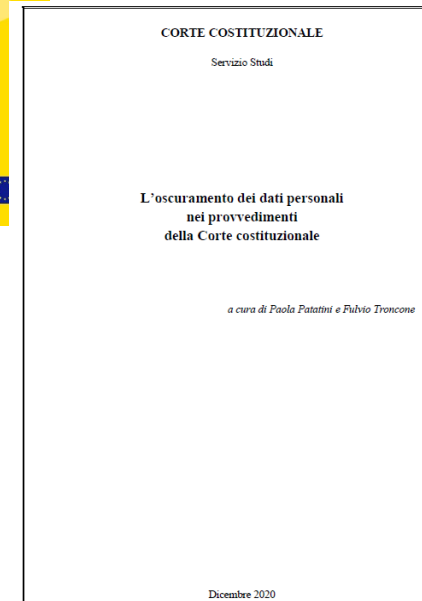


Frequent policies adopted by the courts

- initials of the persons/acronym
- random initials substitution
- substitution with neutral fields e.g., [witness],[victim], [the man's daughter], [telephone number], [victim's address], etc.
- obscure the data
- summary/abstract



Pseudonymization





Pseudonymization – GDPR

Article 4

‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. **The explicit introduction of ‘pseudonymisation’ in this Regulation is not intended to preclude any other measures of data protection.**

Pseudonymization

- Deterministic pseudonymisation
- Document-randomized pseudonymization
- Fully-randomized pseudonymization
- Cryptography

Table 3: Comparison of different techniques in terms of flexibility (identifier format) and pseudonym size

Method	Identifier size	Pseudonym size m in bits
Counter	Any	$m = \log_2 k$
Random Number Generator	Any	$m \gg 2 \log_2 k$
Hash function	Any	Fixed or $m \gg 2 \log_2 k$
Message Auth. Codes	Any	Fixed or $m \gg 2 \log_2 k$
Encryption	Fixed ²⁰	Fixed or same as identifier






WP216- Opinion 05/2014 on Anonymisation Techniques

- “The opinion elaborates on the robustness of each technique based on three criteria:
- (i) is it still possible to single out an individual,
- (ii) is it still possible to link records relating to an individual, and
- (iii) can information be inferred concerning an individual?”

- ***Singling out***
- ***Linkability***
- ***Inference***

ARTICLE 29 DATA PROTECTION WORKING PARTY



0829/14/EN
WP216

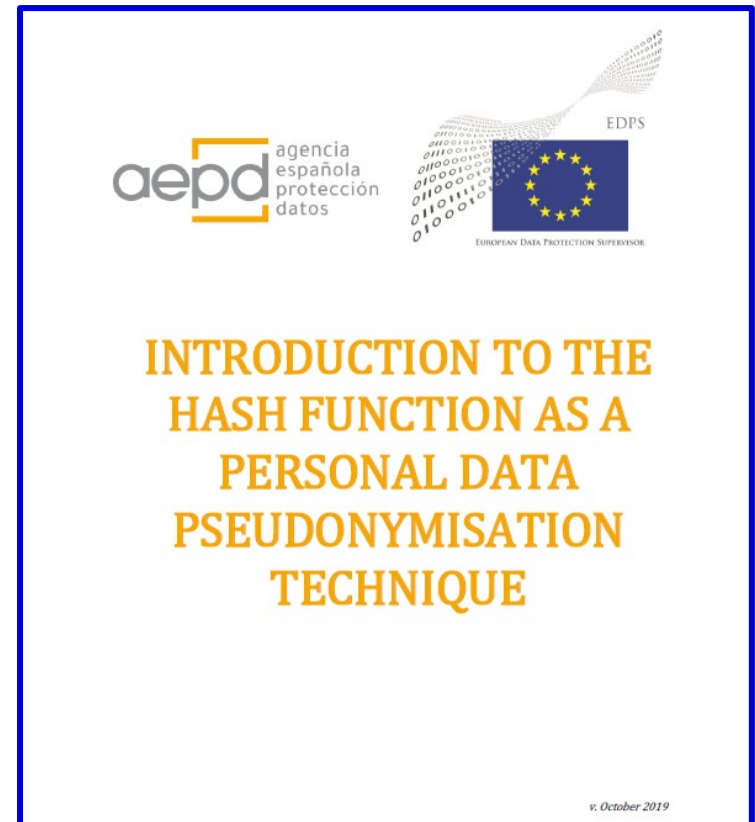
Opinion 05/2014 on Anonymisation Techniques

Adopted on 10 April 2014

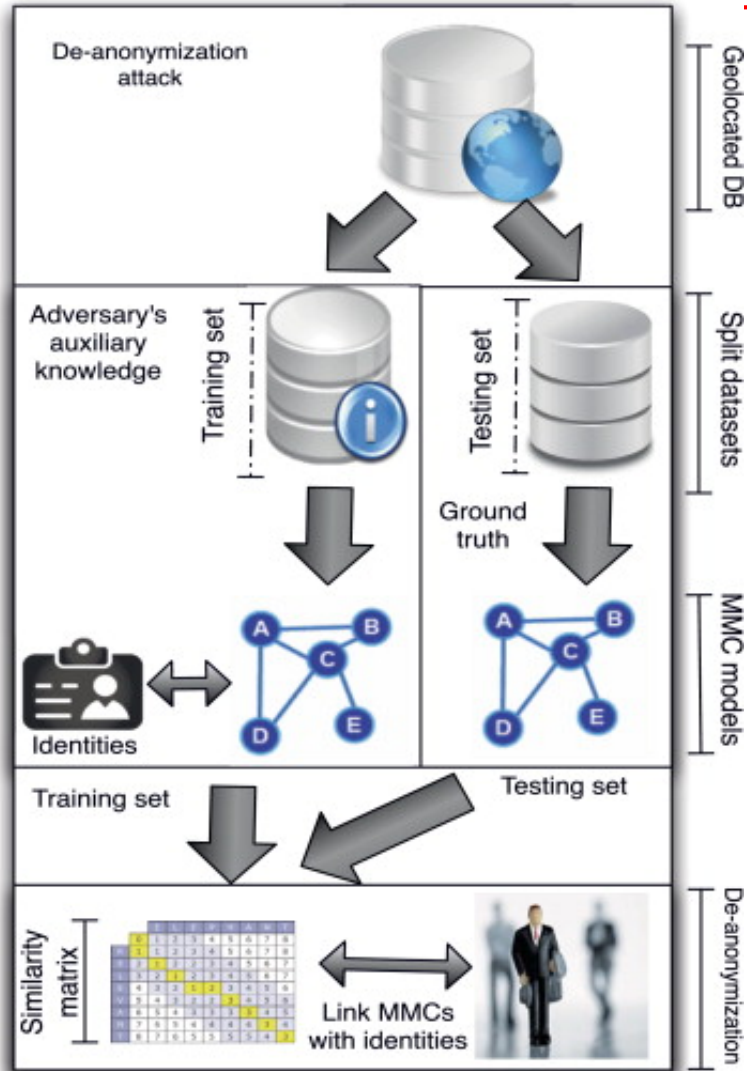


Anonymization/Pseudonimization Techniques

- randomization
 - Noise addition
 - Permutation
 - Differential privacy
- generalization
 - Aggregation and K-anonymity
 - L-diversity/T-closeness
- pseudonymisation
 - Encryption
 - Hash
 - Token
 - Blind Signature



De-Anonymization/Re-Identification



HEALTH DATA IN AN OPEN WORLD

A REPORT ON RE-IDENTIFYING PATIENTS IN THE MBS/PBS DATASET AND THE IMPLICATIONS FOR FUTURE RELEASES OF AUSTRALIAN GOVERNMENT DATA.

Chris Culnane, Benjamin Rubinstein and Vanessa Teague¹,

School of Computing and Information Systems

The University of Melbourne, 18 Dec 2017

{christopher.culnane, benjamin.rubinstein, vjteague}@unimelb.edu.au

[Science](https://doi.org/10.1126/science.1229566), 2013 Jan 18;339(6117):321-4. doi: 10.1126/science.1229566.

Identifying personal genomes by surname inference.

Gymrek M¹, McGuire AL, Golan D, Halperin E, Erlich Y.

Author information

Abstract

Sharing sequencing data sets without identifiers has become a common practice in genomics. Here, we report that surnames can be recovered from personal genomes by profiling short tandem repeats on the Y chromosome (Y-STRs) and querying recreational genetic genealogy databases. We show that a combination of a surname with other types of metadata, such as age and state, can be used to triangulate the identity of the target. A key feature of this technique is that it entirely relies on free, publicly accessible Internet resources. We quantitatively analyze the probability of identification for U.S. males. We further demonstrate the feasibility of this technique by tracing back with high probability the identities of multiple participants in public sequencing projects.

Comment in

Genomic privacy in the information age. [Clin Chem. 2013]

Data re-identification: societal safeguards. [Science. 2013]

PMID: 23329047 DOI: 10.1126/science.1229566

[Indexed for MEDLINE] [Free full text](#)

<https://www.sciencedirect.com/science/article/pii/S002200014000683>



Bill C-11 Canada

- **de-identify** means to modify personal information — or create information from personal information — by using technical processes to ensure that the information does not identify an individual or could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an individual. (*dépersonnaliser*)

Second Session, Forty-third Parliament,
69 Elizabeth II, 2020

HOUSE OF COMMONS OF CANADA

BILL C-11

An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts

FIRST READING, NOVEMBER 17, 2020



Prohibition of re-identification

- **75** An organization must not use de-identified information alone or in combination with other information to identify an individual, except in order to conduct testing of the effectiveness of security safeguards that the organization has put in place to protect the information.
- Fine - \$25,000,000 and 5%

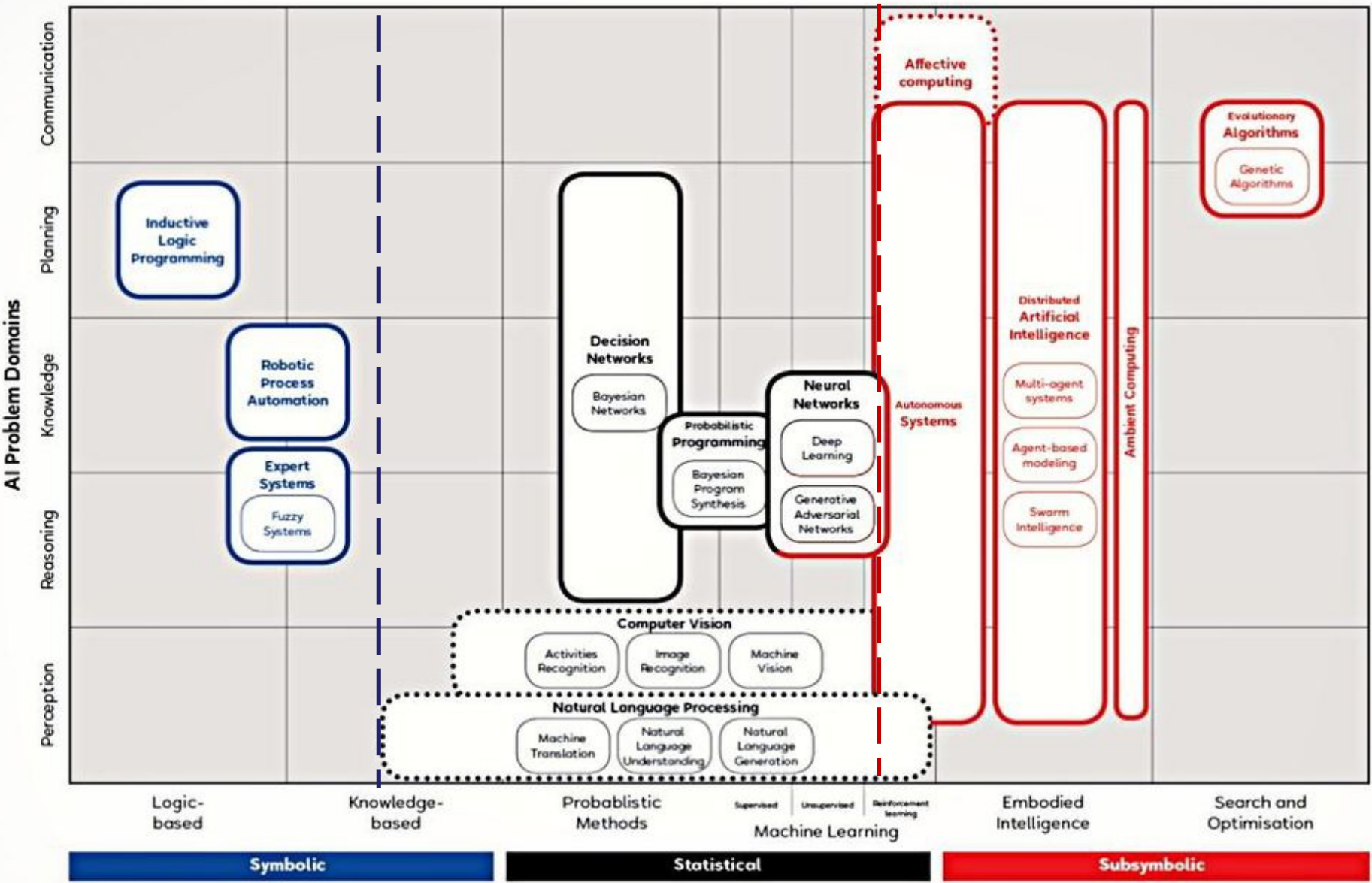


Anonymization/Pseudonymization: an Accountable Dynamic Process

- **Policy**: defines clear rules
- **Detection**: AI techniques could detect personal and non-personal data (NER, ML, DL, DNN, part of speech, etc.)
 - supervised training, accuracy of hypothesis
 - hybrid solutions based on **symbolic** AI and non-symbolic AI should be a good approach
- **Validation**: by human expert
- **Explicability**: to provide a reasonable explanation
- **Anonymization /Pseudonymization**: adopt a robust technique checked periodically (DPIA)



AI constellation



AI Paradigms

Discrimination

<https://algorithmwatch.org/en/story/google-vision-racism/>

Objects Labels Logos Web Properties Safe Search



Screenshot from 2020-04-03 09-51-57.png



Objects Labels Web Properties Safe Search



Screenshot from 2020-04-02 11-51-45.png



Google Vision Cloud April 6th 2020



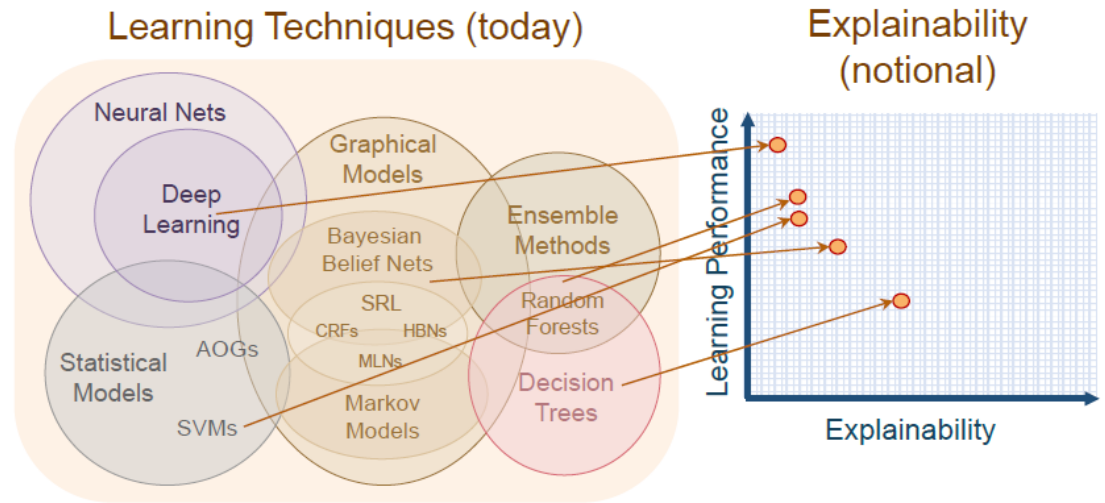
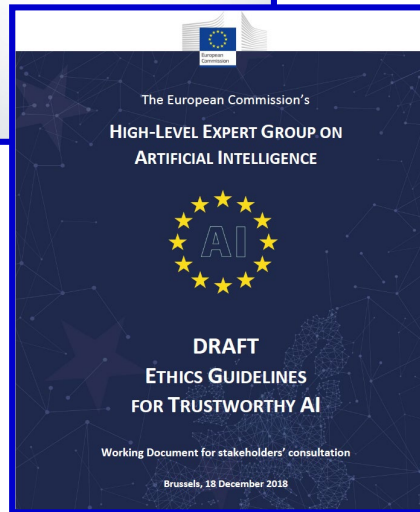
Article 22 Automated individual decision-making, including profiling

1. right not to be subject to a decision based solely on automated processing
2. right to obtain human intervention on the part of the controller
3. right to express his or her point of view and to contest the decision
4. right to explanation

From “right to explanation” to Explicability



Performance vs. Explainability





“White box” approach in AI using LegalXML standard

EasyChair Terms of Service

The EasyChair Terms of Service have changed as part of EasyChair compliance with the GDPR providing a number of new services since the introduction of the previous version of the Terms. To continue using EasyChair you must agree to our new Terms of Service as shown below.

You must agree to our Terms of Service to continue use

You can **download** these Terms of Service by clicking on "Download". To agree to these terms, tick the box below and click on "Continue". If you **disagree** with these Terms [click here to log out](#).

I agree to these Terms of Service

Continue

EasyChair Terms of Service

Thank you for choosing EasyChair!

1. TERMS AND CONDITIONS OF SERVICE

1.1 EasyChair Ltd ("we" or "us" or "EasyChair Ltd"), via its online web service EasyChair ("EasyChair" or "EasyChair Web Site") <https://easychair.org> provides services that allow users

a) to manage document submission, reviewing, publishing, program generation, content management, registration, user management, email management and monitoring, and accounting for conferences, workshops, journals, books, special issues and any other events or publications; and

b) to publish papers, articles, preprints, slides, presentations, videos, teaching material, programs of events, calls for papers and volumes and collections thereof.

(the "Service").

WE ASK THAT YOU READ THESE TERMS AND CONDITIONS OF SERVICE (THESE "TERMS") CAREFULLY BEFORE YOU USE THE SERVICE. BY YOUR ACCEPTANCE OF THESE "TERMS" WITHOUT MODIFICATION, IF YOU DO NOT AGREE TO THESE TERMS, DO NOT USE THE SERVICE.

1.2 If you use the Service on behalf of a company, organisation, or other entity, then

a) "you" includes you and that entity, and

b) you represent and warrant that you are an authorized representative of the entity with the authority to bind the entity's behavior to these Terms, and that you agree to these Terms on the entity's behalf.

1.3 We reserve the right to update the Service at any time at our discretion with or without notice to you. Such updates are designed to improve, enhance and further develop the Service and may take the form of bug fixes, enhanced functions, new modules, or other forms. You agree to receive such updates and permit us to deliver these to you as part of your use of the Service.

1.4 Additional terms may apply to some of our services. For example, if you use our conference registration module, additional terms apply to your use of the module. All of these are referred to below as the "Additional Terms" and further develop the Service and may take the form of bug fixes, enhanced functions, new modules, or other forms. If there is any contradiction between what the Additional Terms say and what these Terms say, then the Additional Terms shall take precedence in relation to that element of the Service.

2.1 We grant you a non-transferable, non-exclusive, non-assignable, non-sublicensable, revocable license to use the Service. It does not include the right for you (or any third party) to copy, adapt, modify, resell or repackage any EasyChair Ltd product, service, or data on the EasyChair Web Site. If you are in contact with us, whether your use is acceptable under these terms, please contact us. The contact information will be available on the contact page of the EasyChair Web Site.

2.2 Your use of the Service does not create a partnership, joint venture or agency relationship or similar relationship between you.

2.3 You are expressly prohibited and shall not, for any third party to reproduce, redistribute, duplicate, copy, sell, sublicense, assemble, modify, sell, lease or re-sell (including the EasyChair Web Site) for any purpose, unless you have been specifically permitted to do so in a separate agreement with EasyChair Ltd.

2.4 No competitors or future competitors of EasyChair Ltd are permitted access to the Service and EasyChair Ltd reserves the right to suspend or terminate any account created or used by any person employed by or acting on behalf of any such competitor.

2.5 You must not use the Service to advertise or promote any fictitious conference(s).

3 YOUR USE OF THE SERVICE

3.1 You represent that you are of legal age to form a binding contract and are not prevented from accessing or receiving the Service under applicable jurisdiction.

3.2 You agree to only use the Service for lawful purposes and as permitted by these Terms.



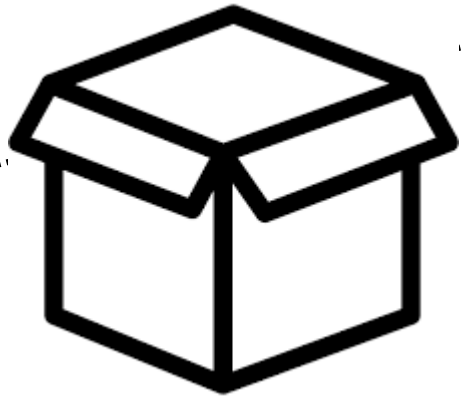
AKOMA NTOSO

Architecture for Knowledge-Oriented Management of African Normative Texts using Open Standards and Ontologies

OASIS LegalXML

LegalRuleML

ECLI



What are your rights in respect of your personal data?

Your right of data access

8.1. You are entitled to receive a copy of your personal data that is in our possession (your right of data access).

Your right to erasure and rectification

8.2 You may request the deletion of personal data or the correction of inaccurate personal data (your right to erasure and rectification). Please note that we may keep certain information concerning you, as required by law, or when we have a legal basis to do so (e.g., our legitimate interest to keep the platform safe and secure for other users).

Your right to object to processing

8.3 You have the right to object at any time (i) to the processing of your personal data for the purpose of direct marketing, or (ii) to the processing of your personal data for other purposes on grounds relating to your particular situation (your right to object to processing). Please note that in the latter case, this right only applies if the processing of your personal data is based on our legitimate interest.

Your right to restriction to processing

8.4 You have the right to restrict the processing of your personal data (your right to restriction of processing). Please note that this only applies if (i) you contested the accuracy of your personal data and we are verifying the accuracy of the personal data, (ii) you exercised your right to object and we are still considering, as foreseen by the applicable law, whether our legitimate grounds to process your personal data in that case override your interests, rights and freedoms; or (iii) your personal data has been processed by us in an unlawful way but you either oppose the erasure of the personal data or want us to keep your personal data in order to establish, exercise or defend a legal claim.

Drafting phase



Machine-readable



Human-readable





Constitutional Court in Akoma Ntoso

CIRSFID, ALMA MATER STUDIORUM - Università di Bologna Sito Cirsfid Sito Corte Costituzionale ITA Accedi all

Pronunce della Corte Costituzionale
Versione Akoma Ntoso a cura del CIRSFID, Università di Bologna

Home Pronunce Informazioni Gruppo di Lavoro

Pronunce Della Corte Costituzionale

Tutte le pronunce della Corte Costituzionale marcate in Akoma Ntoso.

Cosa puoi fare adesso?

- Consulta il catalogo completo in formato Akoma Ntoso nella sezione "[Pronunce](#)".
- Fai una ricerca mirata [cliccando qui](#) oppure sul pulsante di ricerca in alto a destra.
- Consulta le pronunce a partire dalle annate elencate qui sotto.
- Scarica le annate elencate qui sotto nel formato Akoma Ntoso.

Tutte le pronunce per anno

Nel 2019, la Corte Costituzionale ha 2019

Nel 2018, la Corte Costituzionale ha 2018

Nel 2017, la Corte Costituzionale ha

INFORMAZIONI SULLA PRONUNCIA

Sentenza	212/2019
Ecli	ECLI:IT:COST:2019:212
Giudizio	GIUDIZIO DI LEGITTIMITÀ COSTITUZIONALE IN VIA INCIDENTALE
Presidente	LATTANZI
Relatore	Luca Antonini
Data Decisione	2019-07-03
Data Deposito	2019-09-12

Riferimenti Alle Pronunce Della Corte Costituzionale

Riferimenti Alla Legislazione

Conclusions

1. **Balancing** open access with privacy is possible
2. **AI** for detecting the part of speech to manage + **pseudonymization** techniques
3. Dynamic process in the light of **explicitability** and **accountability**
4. Open **LegalXML** standards for Open Justice and minimization of personal data since in the drafting phase of the judgments



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
CAMPUS DI RAVENNA

Monica Palmirani

CIRSFID-ALMA AI, Università di Bologna

monica.palmirani@unibo.it

www.unibo.it