KU LEUVEN CiTiP

CENTRE FOR IT & IP LAW

imec

Transatlantic Perspectives of AI-based Medical Devices Cybersecurity

Elisabetta Biasin

Erik Kamenjašević

KU Leuven Centre for IT & IP Law (CiTiP) – imec

Stanford Law School

Colloquium on cybersecurity in the health sector

28/04/2023 09:15– 9:30 (online)

European University Institute – Centre for Judicial Cooperation

Stanford LawSchool

Contents

Introduction

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

COVID19 | TOPICS | NEWS | PUBLICATIONS

Home > News > ENISA News > Cybersecurity in the healthcare sector during COVID-19 pandemic

News from the same period

- Securing smart infrastructure during the COVID-19 pandemic
- Dependency of Energy Operators on time sensitive services
- Cybersecurity in the healthcare sector during COVID-19 pandemic
- ENISA contributes to a Council of Europe webinar on cooperating with CSIRTs to counter cybercrime
- Sharing is caring: technical cooperation across CSIRTs, LE and the judiciary

NEWS ITEM

Cybersecurity in the healthcare sector during COVID-19 pandemic

ENISA provides cybersecurity advice to support Hospitals and the healthcare sector against the increase of phishing campaigns and ransomware attacks during the coronavirus crisis.

Published on May 11, 2020

EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

Medicines | Human regulatory | Veterinary regulatory | Committees | News & events | Partners & networks

Cyberattack on EMA - update 5

Share

News 15/01/2021

The ongoing investigation of the cyberattack on EMA revealed that some of the unlawfully accessed documents related to COVID-19 medicines and vaccines have been leaked on the internet.

This included internal/confidential email correspondence dating from November, relating to evaluation processes for COVID-19 vaccines. Some of the correspondence has been manipulated by the perpetrators prior to publication in a way which could undermine trust in vaccines.

Two EU marketing authorisations for COVID-19 vaccines have been granted at the end of December/beginning of January following an independent scientific assessment.

Amid the high infection rate in the EU, there is an urgent public health need to make vaccines available to EU citizens as soon as possible. Despite this urgency, there has always been consensus across the EU not to compromise the high-quality standards and to base any recommendation on the strength of the scientific evidence on a vaccine's safety, quality and efficacy, and nothing else.

Hacking healthcare: With 385M patient records exposed, cybersecurity experts sound alarm on breach surge

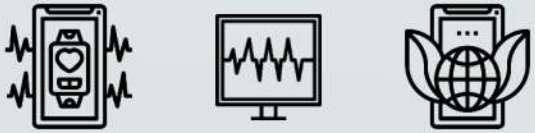
Cybersecurity experts say healthcare companies must harden their defenses, but it may require regulators and lawmakers to raise the bar on security standards.

Published March 9, 2023 · By Samantha Liss and Jessica Vu Han

Cybersecurity of AI-Based Medical Devices

AI

Software as a Medical Device
Medical Device Software



Data Poisoning

Biasin, Kamenjasevic, Ludvigsen (forthcoming, 2023), Cybersecurity of AI medical devices: risks, legislation, and challenges

Social Engineering

Biasin, Kamenjasevic, Ludvigsen (forthcoming, 2023)

Extraction of Data or Source Code

Biasin, Kamenjasevic, Ludvigsen (forthcoming, 2023)

Research Process

Former Research

1. **Medical device cybersecurity**: Framework and challenges with **Cybersecurity Act, Radio Equipment Directive, NIS Directive**

2. **New regulatory challenges**: Cybersecurity of medical devices in MDR vs **AI Act** proposal and **NIS2 Directive** (incident notification & overlaps)

3. **Sustainable Development Goals** and medical device cybersecurity

Current Research

4 **New regulatory challenges**: Cybersecurity of **human enhancement** medical devices in MDR vs **EHDS** proposal and **Data Act** proposal

5 **Transatlantic Technology Law Forum**: Comparative study of legal frameworks for AI-based medical device cybersecurity **(regulatory analysis)**

Relevant EU Legal Framework, Guidance, and Forthcoming Reforms

MD Cybersecurity – Relevant EU Laws

NIS(2) DIRECTIVE	GDPR	AI Act (Proposal)
CYBERSECURITY ACT	Data Act (Proposal)	EHDS (Proposal)

MDR

(+ guidance and soft law)

Shapenlined on Unsplash

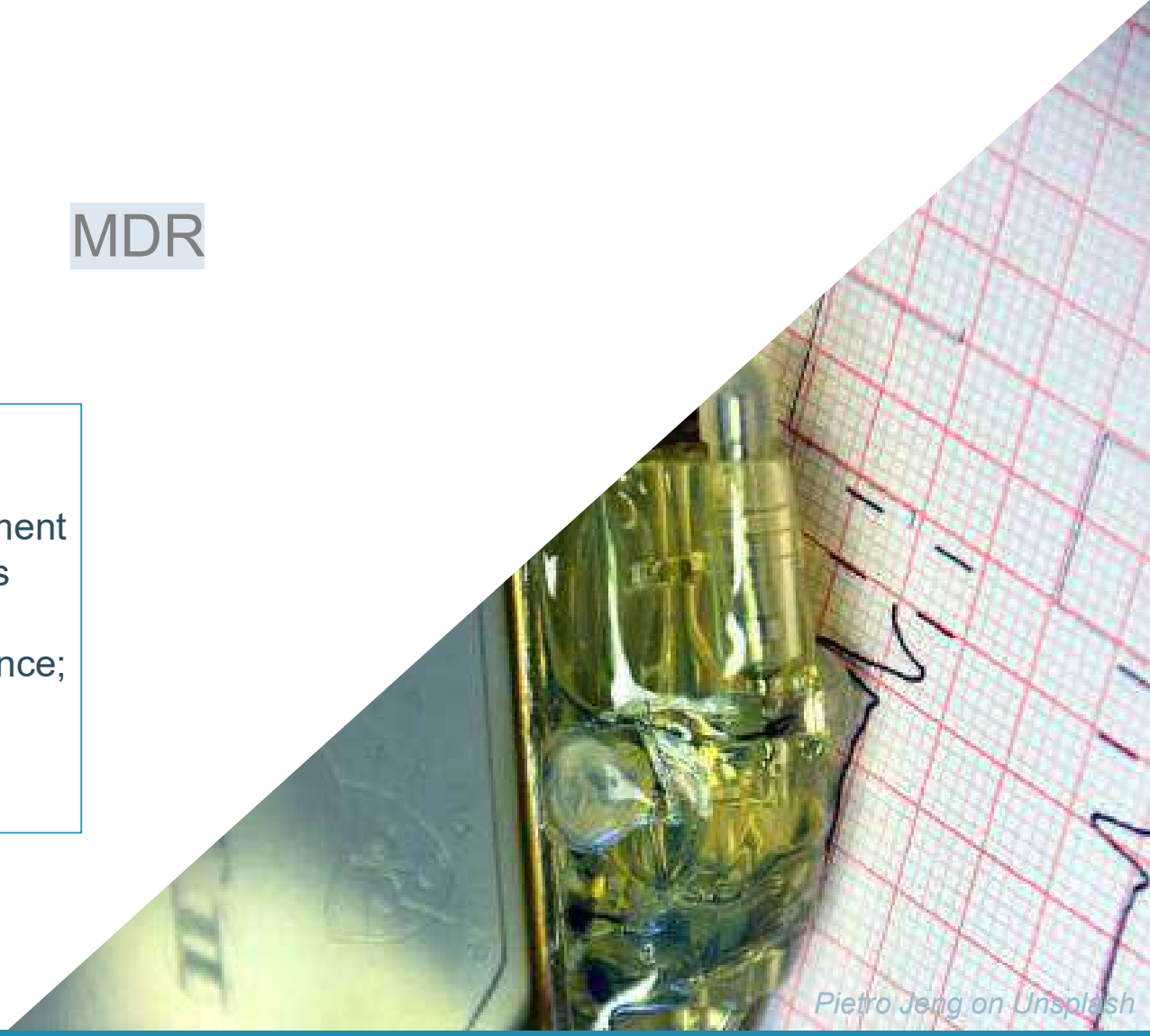
MDR

Safety and performance requirements

Safety and effectiveness; Risk-management system (incl cybersec); design requirements

Software (repeatability, reliability, performance; IT security, IT network, hardware)

Across the whole **lifecycle** of the device



Pietro Jeng on Unsplash

NIS2 Directive

General safety and performance requirements

Healthcare = critical sector
Medical device manufacturers = incl. Annex II

Cybersecurity risk management measures

Reporting obligations

Pietro Jeng on Unsplash

AI Act proposal

May apply to medical devices and safety components thereof

Accuracy, robustness and cybersecurity

Serious incident notification

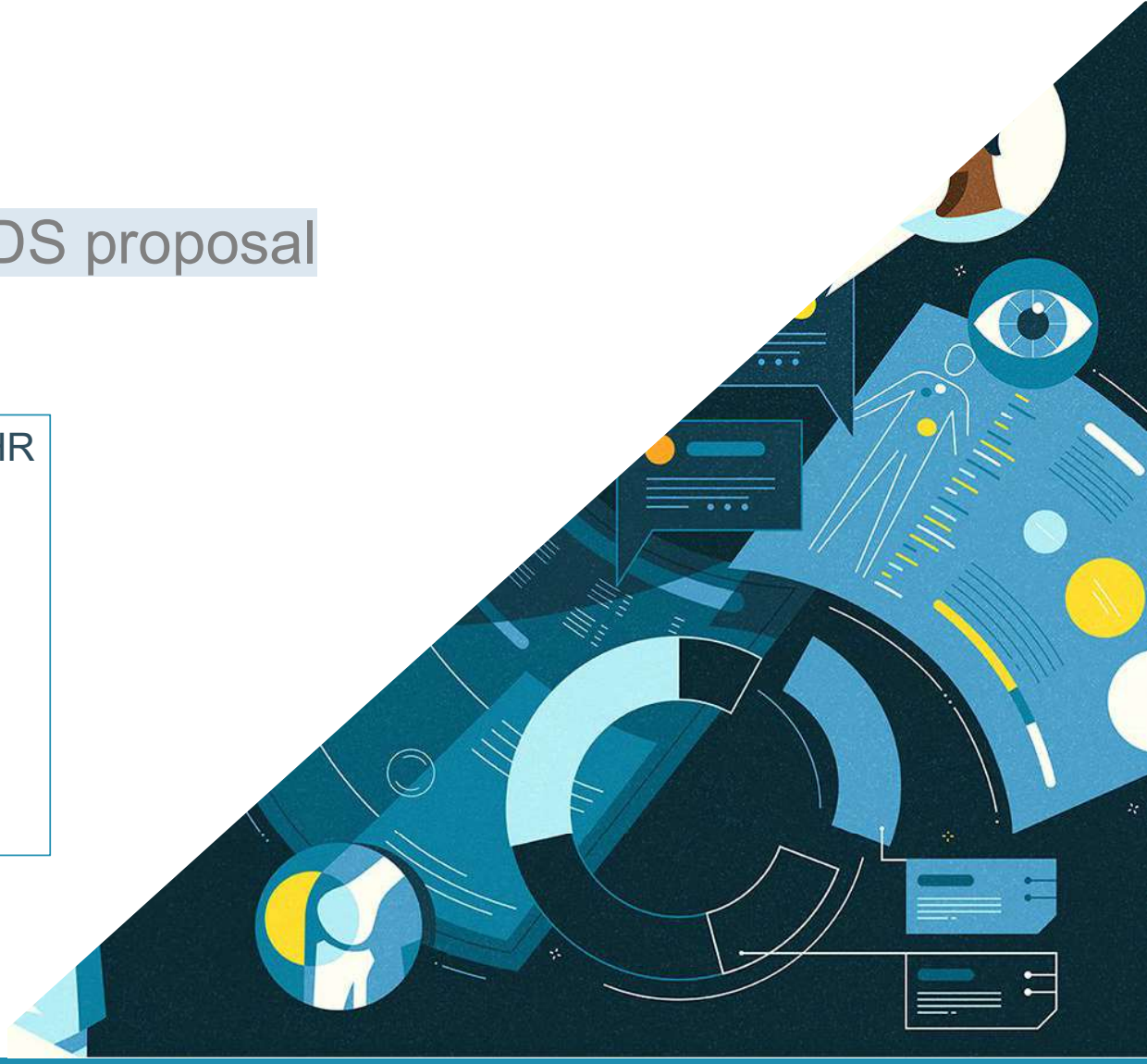
Pietro on Unsplash

EHDS proposal

May apply to medical devices inasmuch EHR systems (?)

Cybersecurity requirements for EHR systems

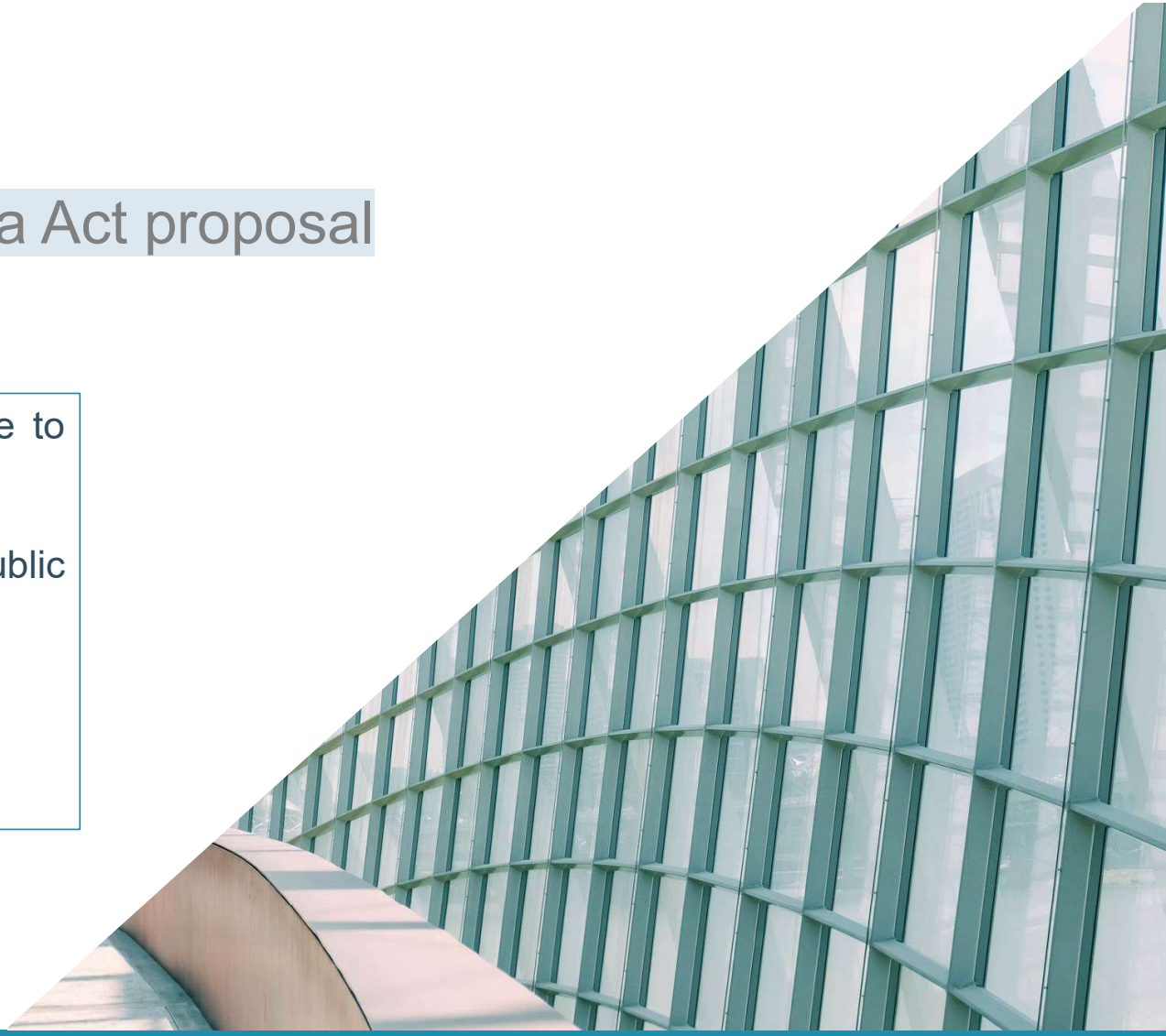
Secure processing environment



Data Act proposal

May apply to medical devices – relevance to business to government data sharing

'major cybersecurity incidents' and public emergencies

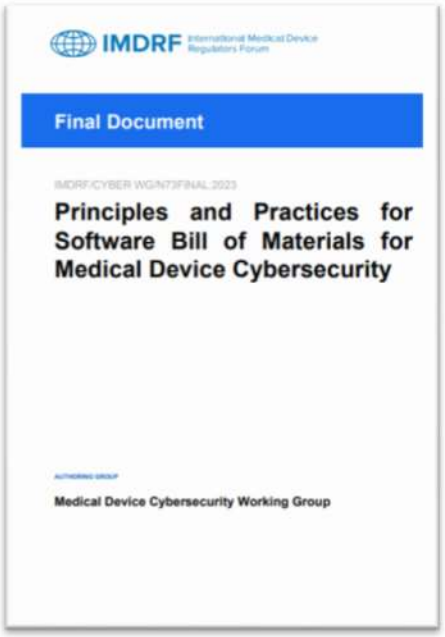


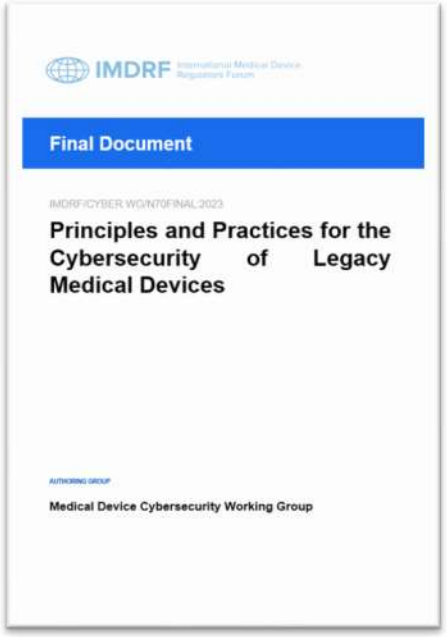
Beyond the EU: International Guidance and Soft Law

National Guidance

- Japanese Pharmaceutical and Medical Devices Agency (2015) Ensuring Cyber Security of Medical Devices in 2015 (PMDA, 2015; 2018; 2022).
- Medical Device Network Security Registration on Technical Review Guidance Principles (2017).
- Germany's Federal Office for Information Security released its Cyber Security Requirements for Network-Connected Medical Devices (BSI, 2018)
- Singapore's Standard Council's technical references on Medical device cybersecurity (SSC, 2018).
- French ANSM guidelines on the cybersecurity of medical devices integrating software during their life cycle; (ANSM, 2019)
- Health Canada's Premarket Requirements for Medical Device Cybersecurity (Health Canada, 2019).
- Australian Department of Health and Aged Care – Therapeutic Goods Administrations guidance documentation (TGA, 2019, amended throughout the years) / consumer information, guidance for industry, and information for users.
- Brazil's health authority principles and practices on medical device cybersecurity in 2020. (ENVISA, 2020).
- Saudi Arabia: initiatives for upcoming guidance (SFDA, 2019).

Supra-national Guidance (IMDRF)





Beyond the EU: the US (focus)

MD Cybersecurity – US references

Section 3305 of the Consolidated Appropriations Act of 2023

General principles for Networked Medical Devices Containing Off-the-Shelf Software (2005)

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (2018)

Guidance for Premarket Submission and Postmarket Management of Cybersecurity in Medical Devices (2014 and 2016)

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submission (2022)

Shapenlined on Unsplash

Preliminary Findings and Conclusion

Literature Review (EU-US)

Medical device law & cybersecurity in the US;

Different legal aspects treated:

- statutory and regulatory gaps on cybersecurity, patient privacy and safety.
- comparison UE-EU cybersecurity requirements.
- broader topic of healthcare cybersecurity; or very specific topic
- Link with critical infrastructure protection;
- best practices; legacy medical devices;
- liability

Medical device law & cybersecurity in the EU

Different legal aspects treated:

- Interplay with other legal acts with cybersecurity requirements
- liability
- cybersecurity certification
- technical aspects
- …
- (ongoing review)

Preliminary Findings

Literature review shows marginal attention to regulation of AI-related aspects and medical device cybersecurity

Regulatory environments have with similarities (risk-based approach)

and differences (FDA vs EU/MDCG/EMA; US vs EU level; device classification; device surveillance)

Next steps: how does these impact to cybersecurity

Thank you!

Cybersecurity of medical devices: Regulatory challenges in the EU

Biasin & Kamenjasevic In I. Cohen, T. Minssen, W. Price II, C. Robertson, & C. Shachar (Eds.), The Future of Medical Device Regulation: Innovation and Protection (pp. 51-62). Cambridge: Cambridge University Press. doi:10.1017/9781108975452.005

Cybersecurity of Medical Devices: New Challenges Arising from the AI Act and NIS 2 Directive Proposals

*

Biasin & Kamenjasevic In International Cybersecurity Law Review. Springer. https://doi.org/10.1365/s43439-022-00054-x)

Cybersecurity of AI medical devices: risks, legislation and challenges

*

Biasin, Kamenjasevic, Ludvigsen, forthcoming
Handbook on AI in healthcare (Soleyman & Cohen eds)

Cyber(in)security of medical devices

*

Kamenjasevic & Biasin, forthcoming, Policy Brief for the United Nations' 8th Multi-stakeholder Forum on Science, Technology and Innovation for the Sustainable Development Goals (May 2023)

Pass the smell test?
The case of human mood enhancement technologies to assess the new cybersecurity-related rules of the AI Act, EHDS and Data Act proposals

*

Biasin, Kamenjasevic, Yasar (forthcoming)

PI: Prof. dr. Anton Vedder
KU Leuven Centre for IT IP Law

Elisabetta Biasin
Doctoral Researcher KU Leuven Centre for IT IP Law

Stanford Law School TTLF Fellow

EMA External Collaborating Expert on Data Protection of Big Data and Real-World Data

Elisabetta.biasin@kuleuven.be

@bisilisib

+32 16 37 77 73

KU Leuven Centre for IT & IP Law (CiTiP) - imec
Sint-Michielsstraat 6, box 3443
BE-3000 Leuven, Belgium

http://www.law.kuleuven.be/citip