Principles: Safety and security, Responsibility and accountability, Awareness and literacy, Multi-stakeholder and adaptive governance and collaboration
Values: Human Rights
Stakeholders: Civil society, Public sector, Technical community

e-Courts in Estonia

At the Estonian Ministry of Justice, a robot judge has been appointed to rule on small claims disputes no larger than € 7,000, the purpose of which is to help clear a backlog of cases for judges and clerks. The online central service system, entitled e-File, provides an overview of the varying stages of the criminal, misdemeanor, civil and administrative procedures, court adjudications, and procedural acts to all parties.

However, as any move towards digitalization, opened Estonia's government to be vulnerable to cyber-attacks in 2007 which is noted as the second largest case of state-sponsored cyberwarfare.

E-File is an integrated system and enables for the exchange of information between all the parties involved in the legal process, from police officers, judges, to citizens. This transition towards an increasingly digitalized legal system has allowed for Estonia to have one of the most effect court systems in the world. One of the more notable benefits to this automated judicial system is the reduced workload of judges and registrars which has allowed them to focus more on complex cases.

The cyberattacks subsequently led to the creation of the NATO Cooperative Cyber Defence Centre of Excellence. Estonia's experiences in 2007 has culminated in the country having one of the most robust cyber security infrastructures in the world with the implementation of scalable blockchain technology.

Artificial Intelligence (AI) has the potential to provide promising outcomes in the judiciary field, for example, through transparency of the functioning of justice, the enhanced support for legal advice and decision-making for litigants. Human error resulting in wrongful convictions is not uncommon in the current judicial system due to human error, flimsy evidence according to the Innocence Project (Innocence Project n.d.). However, numerous jurisdictions, especially in the United States, have begun to incorporate AI tools that can provide recommendations on how to proceed with re-trial detention decisions.

- Developers of the AI systems used by the judiciary need to be cognizant of how the potential for sensitive personal information of netizens to be compromised or leaked and should therefore ensure robust cyber security protection against hackers.

- Judiciary members ensure that there is always a human component involved with any kind of decision-making process. The judiciary sector must also be sure that their IT staff are well trained to deal with cyber-attacks.

- Government should regulate how AI systems are used in court proceedings and educate civil society on becoming more tech literate to ease the transition towards a more digitalized public sector.

Responsibility & accountability Fairness and non-discrimination, Respect and protection of human dignity, safety, and security.

Know more about this case:

- "The Impact of Artificial Intelligence on the Right to a Fair Trial: Towards a Robot Judge?", Asian Journal of Law and Economics, https://www.researchgate.net/publication/343258658_The_Impact_of_Artificial_Intelligence_on_the_Right_to_a_Fair_Trial_Towards_a_Robot_Judge

- "Security and Safety", e-estonia, https://e-estonia.com/solutions/security-and-safety/e-justice/

Additional resources:

- "Toolkit for supporting the implementation of the Guidelines on how to drive towards cyber justice", Council of Europe, https://rm.coe.int/cepej-toolkit-cyberjustice-en-cepej-2019-7/168094ef3e