cyberwatching.eu
The European watch
on cybersecurity & privacy

Emerging technologies in the age of GDPR

Findings and recommendations from European R&I projects

_2020_

Acknowledgements

Cyberwatching.eu is grateful to the projects and individual experts that have contributed to the series of webinars on the topic of emerging technologies in the age of GDPR and to the recommendations provided in this document. More details and contact details can be found in section 4.

Disclaimer

The work described in this document has been conducted within the project cyberwatching.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under Grant Agreement no.740129. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

Table of Contents

Acronyms

AI	Artificial Intelligence
ANASTACIA	Advanced Networked Agents for Security and Trust Assessment
COO	Chief Operating Officer
CREATE-IoT	CRoss fErtilisation through AlignmenT, synchronisation and Exchanges for Internet of Thing
DLT	Distributed ledger technology
DPO	Data Proection Officer
EU	European Union
GDPR	General Data Protection Regulation
IdP	Integrated data processing
IoT	Internet of Thing
mF2C	Towards an Open, Secure, Decentralised and Coordinated Fog-to-Cloud Management Ecosystem
MHMD	My Health My Data
ML	Machine learning
MIT's ENIGMA	Massachusetts Intitute of technology's decentralised open-source protocol
PRIViLEDGE	Privacy-Enhancing Cryptography in Distributed Ledgers
P-ABC	Privacy and distributed Attribute-Based Credentials
R&I	Research and Innovation
SDWAN	Software-defined networks in a large area
SOFIE	Secure Open Federation for Internet Everywhere
VPN	Virtual Private Network
ZKP	Zero-knowledge proof

1 Introduction

1.1 Cyberwatching Concertation and Webinars on Cybersecurity

Three of the most recurring topics during the second (2nd) cyberwatching.eu Concertation last June 2019[1] in Brussels were AI, IoT, and Blockchain. Aside from recommendations delivered to the European Commission with regard to the Horizon 2020 and Digital Europe Programme in our report *EU cybersecurity legal and policy aspects* (D3.4)[2], the cyberwatching.eu consortium organised two webinars in the last quarter of 2019 to address the issues. Several R&I projects collaborated and participated in addressing the challenges and opportunities in the Blockchain and IoT era:

- "Blockchain: multi-application viewpoints and opportunities"[3] with the participation of **SOFIE**, **PRIViLEDGE** and **MyHealthMyData** (MHMD).
- "The Cyber Security Challenges in the IoT Era"[4] with the participation of R&I projects such as **mF2C**, **CREATE-IOT** and **ANASTACIA**.

Based on experience with their platforms and use cases, the projects identified several current and future challenges as particularly "interesting".

In this report, six (6) research and innovation (R&I) projects related to cybersecurity and privacy collaborated with cyberwatching.eu to provide a consolidated overview of the most significant barriers in the area of cybersecurity and privacy with respect to these three technology/technological applications and lay down concrete recommendations on these matters will be proposed.

1.2 Security and Privacy in Modern Society

Data is more important than ever today, both in individual and societal terms. The two major concerns surrounding our data today are:

- **Security**. Protection against intrusion, hacking, and the integrity of our data.
- **Privacy**. Protection of the confidentiality of our data and its misuse by others.

Emerging technologies can boost performance and productivity for organisations across Europe boosting performance, productivity and the European Digital Single Market.

However, even while promising new opportunities for innovative uses of our data, these technologies also present threats both to their security and their privacy. AI and Blockchain pose threats to privacy. The Internet of Things adds a significant threat to security.

At the same time, Europeans have set high standards for digital privacy. The GDPR now enforces stricter regulations on data handling and processing. But this may make it more difficult for organisations reap the benefits that these technologies deliver through massive data and high-quality algorithms and at the same time be GDPR compliant.

1.2.1 Security: A constant threat in modern society

There is no need here to repeat the many headlines that are appearing around the world today on cybersecurity: hacking, ransomware, and much else is a constant threat to the very fabric of our society. Technologists must confront the threat with the best practices available. Security-by-design is an approach to constructing systems with secure characteristics "built in". This involves

[1] https://www.cyberwatching.eu/news-events/events/brussels-second-cw-concertation-meeting-04062019-0

[2] https://www.cyberwatching.eu/d34-eu-cybersecurity-legal-and-policy-aspects-preliminary-recommendations-and-road-ahead

[3] https://www.cyberwatching.eu/blockchain-multi-application-viewpoints-and-opportunities

[4] https://www.cyberwatching.eu/cyber-security-challenges-iot-era

a number of principles that have been proven effective over the years. Together with other principles such as “defence in depth”, these constitute a body of knowledge about secure systems design that is now quite mature and ready to disseminate to system builders throughout Europe.

1.2.2 Privacy: The General Data Protection Regulation

The General Data Protection Regulation (GDPR) entered into force on 24 May 2016 and is applicable since 25 May 2018. It represents European leadership in privacy protection. Its principal characteristics include the following:

Well-defined terminology. Individuals are **data subjects** in the GDPR. A **data controller** is Any organization, person, or body that determines the purposes and means of processing personal data. A **data processor** processes the data on behalf of the data controller.

Principle of transparency. Being informed about how the data is being used; being informed on how the processing works (e.g. the algorithm), and who is doing the processing.

Principle of restricted use. Use only for the purposes for which the data was collected.

Permission to lawfully process third-party data. Although GDPR does not prevent a third party acting on behalf of an individual to indicate their consent. But the third party must have the authority to do so. This is not always a simple matter.

The right to rectification or erasure. Also known informally as “the right to forget”, it is the right to have your personal data deleted.

As we will see in the following, the emerging technologies present challenges to all of these principles.

2 The Challenges of Emerging Technologies

2.1.1 Artificial Intelligence

AI in the age of the GDPR. Artificial intelligence (“AI”) is an undeniable component of the future of technology and cyberspace, which can be implemented in the systems, software and devices of different sectors.[5] From a data protection perspective, AI is typically utilized as a tool for automated decision-making and profiling, by leveraging algorithms to process a large volume of data.[6] The challenges arise where the processing done by the AI is of such a nature that it creates significant effects for the data subjects.

Firstly, the principle of transparency is at stake. When controllers use AI as a tool to process personal data because the data subjects may not be sufficiently informed about the way in which their personal data is being collected and processed. The reason for this is that, when it comes to AI, proper/full information about processing data cannot always be given. As a matter of fact, if a controller uses AI it may be quite challenging to strictly define how the personal data will be processed and for which purposes exactly, given that a machine learning algorithm has, per definition, a behaviour that changes (learn) over time in terms of actions on the data, correlations drawn, and outputs (that can affect an individual). Therefore, it becomes hard to give prior information notice to data subjects when the content of that notice may be dependent on the result of the AI decision making. As can be seen, **there is a circular process that would allow for**

[5] Guidelines on Artificial Intelligence and Data Protection, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 25 January 2019.

[6] Big Data, Artificial Intelligence, Machine Learning, and Data Protection https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

those utilizing AI an additional requirement – in which the data subjects whose personal data is being processed must receive additional information as the AI comes to conclusions. However, as per the current legislative framework of the GDPR – this has not been envisaged. The information notice, as per Article 13 and 14 GDPR, must include all information regarding the processing, and where the processing includes automated decision making, it must also include the logic of the algorithm and the impact that it may have on the data subject. Therefore, **a solution must be given for the AI models that process personal data by means of machine learning algorithms that may change the logic and the impact on individuals over time**.

Related to the previous challenge is the fact that **the machine learning algorithm may in fact autonomously (and in an unexpected/unpredictable way) process personal data of individuals for purposes different or incompatible with the ones for which the data were collected**. Essentially, this would mean that the AI has already processed personal data of that person, for a purpose which was not originally disclosed or that it is incompatible (see Art. 6(4) GDPR). Therefore, the controller and, therefore, the data subject are not in control anymore of how the data are processed. This is a challenge that seriously undermines the entire rationale behind the protection of personal data.

Furthermore, **the risk assessment of the automated processing conducted through AI may be in several cases unrealistic**. For the reasons outlined above, the risk of the processing, as well as the envisaged consequences for data subjects, may not be comprehensively analysed beforehand by the controller (in contrast with what is required by Art.s 24 and 24 GDPR). Therefore, the risk-based approach would be severely undermined in processing activities relating to AI. This may also lead to a case where the security measures that may have been implemented originally, are no longer adequate (see Art. 32 GDPR), considering the evolving circumstances of the processing activities.

2.1.2 The Internet of Things

IoT in the age of the GDPR. The Internet of Things ("IoT") is another emerging technology that poses challenges to the European framework for data protection. The opportunity for the economy and society to have an ecosystem of interconnected services and devices is undoubted. However, the amount of personal data that is collected through the sensors of these IoT devices or services is both large and inherently intrusive.

The first concern in the realm of IoT devices and services is the principles of data protection by design and by default and data minimisation. In complex IoT environments, designing data flows aimed at minimising the use of data and preserving individual privacy to the maximum extent without diminishing the functionalities of the systems is a great challenge. Moreover, assuring end-to-end security during the entire data-lifecycle is a clear issue given that the machines performing data processing are typically under the control of different organisations (acting as controllers or processors as the case may be) without an overarching orchestration and control over the data. **There is a need for further guidelines on the application of the principles of data protection by design/default and data minimisation for IoT deployments**.

Additionally, **in an IoT environment users may struggle to receive meaningful and complete information regarding the relevant data processing activities (see Art.s 12-13-14 GDPR)**. Usually, IoT-related data processing happens without an effective user knowledge and/or understanding of it. There is no clear and comprehensive information point where users can understand how data are processed in the IoT environment and by whom. In such a situation, furthermore, the IoT devices may inadvertently collect personal data of data subjects who may not have consented to that processing of their data; such as visitors of smart homes/offices. **In this case, the principle of transparency becomes significantly challenged and the solution does not seem to have been taken into account within the GDPR.**

This last point also brings up the **issue of lawfulness** of the processing of personal data of visitors or data subjects that may not be the primary IoT user. A detrimental component of processing personal data is that it may give rise to the risks of sanctions for IoT services that do not have a legitimate legal basis to process personal data of third parties or other persons that may neither be informed of the processing nor be given the change to consent or object to it. **This challenge is closely related to the data subject's rights**, which it can hardly be argued, are able to be exercised. In fact, if a data subject is not adequately informed of the IoT processing their personal data, then it follows that they will also not be offered an appropriate method to exercise their rights as data subjects.

Lastly, **IoT poses strong challenges to the allocation of privacy roles**. For example, IoT data processing is often carried out by machines managed by different organisations, each of them using computational capacity provided by cloud service providers and that can also involve analytic software programmes supplied by the related vendors. This exponentially increases the number of parties involved in the data processing activities and to clearly allocate the privacy roles in terms of controller, processor or joint- controller. Failing to correctly identify the roles will result in a possible misallocation of respective duties and obligations towards the data subjects and towards the competent Supervisory Authorities. Additionally, when the parties to a processing activity of IoT deployments are so numerous, it is not realistic to expect that all controllers will legally bind their processors. However, the GDPR clearly requires, through Article 28(3), that a contract or other instrument must be signed between the controller and the processor. **Practical guidelines should be given in the allocation of privacy roles in IoT environments in the light of the GDPR**.

The Projects Speak.

Several of the projects contributed observations and recommendations on aspects both of IoT privacy and security. The **mF2C**[7] project contributed a number of reflections:

Hardware security at the edge. Edge devices might be exposed to tampering, particularly if they can be temporarily powered down. In general, it is very difficult to protect against a very resourceful attacker, and increasingly expensive. It is necessary to have a scale of edge physical security – including a simple switch which can detect whether a device has been opened to tamper-evident potted circuit boards. The particular challenges include improving the cost-effectiveness of existing protections and making devices protect themselves (as opposed to being inspected for tampering) when they might be temporarily unpowered or temporarily disconnected from networks.

Updating edge devices. When devices are deployed, it makes sense to be able to update their firmware/software/keys from time to time. Obviously, this is only sensible if only authorised updates are installed – it would not make sense if an attacker could update the firmware as well. The IoT industry has a range of solutions for this, and it would make sense to work with these. Other edge devices, like smart phones and devices running containerised services, would be able to update themselves as long as they have connectivity to a trusted repository.

Based on this, the challenge is to support a range of devices with different means of updating. For many devices, connecting to a trusted repository, or relaying updates through other devices with connectivity, would make sense, but may be expensive. For others, updating the device physically would make more sense, particularly if there is risk of tampering. Yet other devices might not be updatable at all, and need to self-destruct (as it were) when they become vulnerable.

Overall user experience (usability) and managing users as the "weak link". Security is often the antonym of usability – much work has gone into the rightly maligned passwords, and often users would choose the lesser security setting to get increased convenience or functionality (think of browsers). In traditional e-infrastructure security, there are a few win-win scenarios, such as using federated identity management which, if applied correctly, can improve both usability and the level of assurance, compared with username/passwords. For user-managed edge devices, it makes sense to identify and support similar win-win scenarios, and/or to support a security scale depending on the risk introduced by the device.

GDPR support. A related topic is giving users control of their data, or at least visibility of how it has been processed. This is obvious – it's a legal obligation – but focus has (rightly) been on

[7] https://www.cyberwatching.eu/projects/1078/mf2c

informing users prior to the processing. As the next step, we would be interested in giving users insight into how the data was actually processed – which can be more specific than the initial declaration by the service – and where it is currently held.

Managing IoT with legacy devices. The new devices that we produce are not alone – they join a plethora of existing IoT devices along with many other things on the network. Compromise of legacy devices could affect the functionality – networking, in particular – of more recent devices. The mF2C project looked briefly at updating firewalls and routers in response to an incident, but it was an early proof of concept. It would be essential to respond in an automated fashion – perhaps a machine learning approach – in order to minimise the risk. Of course, one then needs to make sure that an attack is not confused with an emergency – we want the system to protect itself against an attack but still handle the emergency correctly.

Virtualisation for edge device security. The mF2C platform is implemented using containers (with Docker). Containers can add security features – such as private networks and isolation of ports and file systems but can also hinder security if the container user has too many privileges, or kernel vulnerabilities affect the container. Combined with network security, there is an opportunity to build on these existing tools and make them mature and integrated into an IoT platform. mF2C uses VPN secured with certificates, but this could be extended to more advanced virtualised networking. We also know the industry is keen on providing SDWAN “solutions”.

The **ANASTACIA**[8] project contributed an observation together with a recommendation on the problem of security incident data sharing in the Internet of Things:

Intelligent Management of Incident and Data Sharing. Many users are reluctant to openly share data about security incidents (either through embarrassment or concern about damage to corporate image). If privacy and anonymity could be guaranteed, the rate of contributions would increase significantly.

Even though interoperability across multiple service providers could be accomplished using a single identity provider, this is not enough to protect users’ privacy. Indeed, an IdP that generates tokens that prove users’ identities for their online and offline transactions can track said users’ activity, learning which services they interact with and when these interactions occur. To combat this, there arises the challenge of creating a distributed oblivious identity management system. Such a system may rely on distributed cryptographic techniques to split up the role of the online IdP over multiple authorities so that no single authority can impersonate or track its users.

Additionally, it is expected a decentralized identity and ensures interoperability that could help on supporting a Privacy and distributed Attribute-Based Credentials (P-ABC) and a distributed oblivious identity management system with cryptographic techniques to split up the role of the online IdP over multiple authorities. The system architecture and the cryptographic tools needed to perform said role distribution will be the baseline of the challenge.

Finally, the **Create-IoT**[9] project has concentrated on data protection, privacy and certification, and contributed a number of suggestions that future funding initiatives from the European Commission could take into account in these areas. The recommendations listed specific challenges in security and privacy in the IoT that would be particularly relevant to address:

- citizens, public authorities and companies, including SMEs, need to be empowered to protect their data and online activities;
- human aspects in cybersecurity should be reinforced;
- data sharing models and policies;
- privacy on data sharing;
- threat modelling, data flow modelling, characterization of systems and assets (safety, legal, economic);
- role of certification under the GDPR and the EU Cybersecurity Act;

[8] https://www.cyberwatching.eu/projects/934/anastacia

[9] https://www.cyberwatching.eu/projects/1556/create-iot

- comparison of the level of data protection offered by the GDPR with other jurisdictions such as U.S., India, South America;

2.1.3 Blockchain

Distributed Ledger Technology in the age of the GDPR. It is also very important to address the matters raised by the GDPR when considering the use of blockchain-based systems, as not only do they offer the possibility for personal data to be directly recorded 'on-chain', but also require the use of personal data (in the form of public keys/identifiers) for their very functioning. Given the high standard for anonymisation set by the Article 29 Working Party, even encryption or irreversible hashing of personal data stored on the blockchain will not suffice to circumvent the discussion (at least, for now).

The interaction between blockchain and internationally recognised data processing principles is not always smooth. **While some principles remain largely unaffected by the technology, such as the principle of lawfulness and purpose limitation, and others may even find themselves enhanced by the additional functionalities brought about by blockchain, such as the principle of fairness, others still appear to frontally collide with its 'set-in-stone' nature, namely the principles of data minimisation and storage limitation which, in turn, may affect the ability to effectively exercise some data subject rights regarding personal data stored 'on-chain' (such as the right to rectification or erasure).** It is also not a simple matter to identify and agree on the **data processing roles** played by the participants in a blockchain-based system. **An even more complicated matter is to ensure that the formal requirements tied into these roles are met, such as the need for a contract or other legal act containing a set of minimum obligations to be entered into with each processor engaged by a controller, in light of Art. 28 GDPR – this problem currently appears not to have a practically viable solution when considering public blockchains**. The matter of **international transfers** and the implementation of the requirements for their lawfulness raises similar difficulties in light of the decentralised nature of blockchain-based systems.

In general, many of these issues can be solved by storing personal data in an 'off-chain' solution, and merely referencing those data (e.g., via a commitment or hash pointer) within the blockchain-based system itself. However, in any case, it must be understood that, while blockchain has the potential to allow individuals to retain control of their data and even to understand, in a transparent manner, who has access to their information and to what extent, this by no means results automatically from the use of blockchain-based systems to process personal data. Rather, those systems must be specifically crafted, in careful consideration of the rules set by the principles of data protection by design and, specifically, of fairness by design, to ensure that individuals' privacy and real control over their data is afforded to them.

The use of blockchain technology as a means to process personal data has been called into question ever since the GDPR was first announced, with doubts solidified by the European Parliament's stance on the matter. For now, it seems that there are manners in which to handle the potential objections raised, at least where private or permissioned blockchains are concerned.

Practical clarifications on the application of the GDPR to blockchain are very much needed for this technology and the law to coexist.

The Projects Speak.

Funded projects have been particularly active in advancing Distributed Ledger Technologies, and the projects were eager to contribute their observations based on experience gathered over the duration of their activities.

The **PRIViLEDGE**[10] project contributed its point of view on the GDPR and privacy in DLT:

Privacy in the context of distributed ledger technology. Blockchain is a distributed ledger that maintains the integrity of transactions, it is one potential building block for applications that require

[10] https://www.cyberwatching.eu/projects/1033/priviledge

such integrity preserving, verifiable (potentially generally public) ledger of certain transactions. For some applications, the data published on the ledger is also subject to privacy requirements. In electronic voting we must have the capability to verify the correctness of the tally and at the same time keep individual preferences of the voters' secret. Although there is research taking place and there exist cryptographic tools to implement privacy-preserving protocols on top of DLT, these methods are not straightforward and call for application domain-specific protocol design.

The **SOFIE**[11] project contributed observation on several different aspects of Blockchain, also based on concrete use case experience in the project:

Cascading effects to the energy networks and mitigation actions. Given the current strong interconnection between electricity/gas controlling systems, and the fact that the stability of the grid at EU level depends on the whole integrity of the network for the EU (and beyond), cascading effects upon a cyberattack on a particular region are a huge risk for causing a failure at large scale due to a domino effect. Blockchain technology and distributed ledgers could help to mitigate these risks but it needs to be assured that the right tools and capabilities are used for this. An approach (which requires attention) is to test various combinations from new technologies in action. Utilizing multiple ledgers that are interconnected through inter-ledger functionality instead of a single DLT provides the flexibility to exploit the aforementioned tradeoffs. Finally, providing inter ledger mechanisms to interconnect different DLTs allows companies and consortiums to select private/permission distributed ledgers based on their requirements and constraints. Hence, inter-ledger mechanisms can enhance interoperability across different IoT platforms that utilize different distributed ledger technologies.

The result would be seamless information sharing with the trust and traceability features enabled but overcoming the well-known challenges of using only private or public Blockchains/DLTs (scalability, challenges with consensus mechanisms, immutability).

Challenges of legacy technology combined with new technology. Energy systems combine legacy equipment, in some cases installed decades ago and not prepared to deal with cybersecurity, with state-of-the-art new digital equipment following the security-by-design principle, but commonly exposing some of the legacy equipment to unforeseen digital threats. In addition, the incorporation of IoT devices into energy systems leads to additional risk. Most of these devices are not compliant with the strict requirements for the security of energy networks and there is a high risk of malicious usage when connecting them with no security or trust assurance. There is no one single solution to this challenge. One path is to have the energy networks include application-level security measures, such as user authentication and role-based access control, in addition to measures of telecommunication networks adapted to the operational context, such as firewall, intrusion detection systems, hop authentication and data encryption. From the user authentication and role-based access control, decentralised identifiers and a combination of Public Key Infrastructure and blockchain-based certificate handling (Decentralised Identifiers) could be investigated.

The integrity of data and provenance chain for AI, big data analytics and machine learning. One of the main features of blockchains and DLT is the means to prove the integrity of data and processes. With the rapid growth of both input data and the complexity of the processes that are run on top of it, it is crucial that the control over the data and processes remains in the hands of the operator (the one requiring the results for business decisions). This means that in parallel to innovation and research in these popular domains (AI, Big Data) the tools for integrity verification on a massive scale should be developed.

Finally, the **MyHealthMyData**[12] **(MHMD)** project made numerous contributions on yet more aspects of the difficult problem of DLT management:

Focus on interoperability of different blockchain solutions. Focus on interoperability of different blockchain solutions (and relevant standardisation activities) for specific kinds of data. This is very relevant for critical services such as healthcare, where it is of paramount importance

[11] https://www.cyberwatching.eu/projects/1302/sofie

[12] https://www.cyberwatching.eu/projects/1479/myhealthmydata-mhmd

to ensure finality of transaction in a time-sensitive manner. This means that – from the end-user perspective – the information exchange should be guaranteed to take place, within a guaranteed amount of time, no matter what the underlying blockchain service provider is (assuming – as is foreseeable – that we will have eventually multiple blockchain providers and services). The idea is ensuring resilience and continuity of service beyond individual technical architectures.

Explore distributed data storage solutions in the sensitive domain and the relevant impact on the regulatory framework. The future of data storage is not in siloes, but rather distributed throughout a number of different locations. This means enhanced security and user control (as each data storage provider would only hold a piece of data and only the data owner could gather up all the pieces to reconstruct the original data). At the same time, this will have an impact on the regulatory framework associated with data storage, management, control and agency.

Explore the creation of high-level and advanced smart contracts libraries and their legal and technical implication. Explore full operational applicability of smart contracts in establishing and executing peer-to-peer agreements, also including the possible combination between smart contracts and Ricardian contracts (the former devoted to the execution of the operational clauses of an agreement (if-then logic) and the latter mostly concerned with the process of completing the agreement in a non-repudiable and clear way for all involved parties. A sub-topic of this is the exploration of smart contract templates and specific languages (including natural smart contract language allowing to compile a smart contract in natural language and ensure its effective transformation in the corresponding code, whatever the ending-point technical language might be – i.e. Go, Java, Solidity, etc.). Also explore trusted coding and/or execution environment for smart contracts and relevant public auditing services. Another subtopic can be the combination of smart contracts (and more in general blockchain) with Zero Knowledge tools and other privacy-preserving tools.

Explore automated tools for assessing infrastructure reliability. There is a need for tools/methodology capable of verifying/auditing the claims about validity of (novel) consensus mechanisms, immutability of the ledger, performances, scalability, confidentiality, correct functionality of smart contracts. At the same time, tools are also necessary to assess the needs of blockchain solutions in terms of scalability and energy efficiency, answering questions like “What levels of global distributed consensus are actually required for certain use cases?” and “what are the relevant inherent costs for reaching those levels of consensus in a reliable and secure manner?”). a sub-topic could be the study of hybrid blockchain and federated blockchain, providing clear proof-of-concepts and performance assessment (in particular in terms of consensus, tamper-proof features, reliability…).

Focus on the concept of synthetic data. Focusing on the concept of synthetic data (i.e. data created starting from real databases but no longer linked to any real individual), for going beyond security and privacy in privacy-sensitive data handling and analytics domain, also allowing to provide AI developers with a wealth of new data to use for ML training and validation.

Explore more in detail the recent trends in federated learning and computing. The relevant concept of bringing algorithms to data, for reduced cyber risk and advanced privacy. Much experience has been gained in the past few years (ZKP, Homomorphic encryption, Secure Multi-Party Computation, MIT’s ENIGMA, etc.), but the field still needs research resources to move forward to practical and viable applications in real world scenarios.

3 Conclusion

The main recommendations from this document are detailed below.

AI:

- **Focus on transparency of AI algorithms**. Probably the most serious challenge to the use of AI in privacy-sensitive activities is represented by new technologies such as Machine Learning, which can make it nearly impossible to track the inner workings of algorithms. Support research in "self-explaining AI" techniques in order to confront this issue.

Blockchain:

- **Focus on interoperability**. Different blockchain solutions will be with us for many years to come, and they must be interoperable.
- Explore smart contracts. They have much to offer and will open up many opportunities.
- **Consider distributed data for privacy preservation**. Distributing the key elements of privacy-sensitive data is a promising approach to keeping the sensitive data out of the hands of a single actor.

IoT:

- **Have a scale of edge physical security** – including a simple switch which can detect whether a device has been opened to tamper-evident potted circuit boards.
- **Don't forget legacy systems.** IoT has the particular challenge that many legacy systems are integrated, representing a major technological challenge to preserving cybersecurity and privacy.

4 Contributing projects

Cyberwatching.eu would like to thanks the projects and representatives that have contributed to this document.

- **ANASTACIA**, http://www.anastacia-h2020.eu/

  Contributor: Dr Antonio Skarmeta
  Scientific Coordinator, WP2 Leader
  University of Murcia

- **CREATE-IoT**, https://european-iot-pilots.eu/project/create-iot/

  Contributor: Dr. Pasquale Annicchino
  Qualified Associate Professor of Law, DPO
  Archimede Solutions SARL

- **mF2C**, https://www.mf2c-project.eu/

  Contributor: Dr. Jens Jensen
  Principal Scientist
  UKRI-STFC

- **MyHealthMyData** (MHMD), http://www.myhealthmydata.eu/

  Contributor: Mirko De Maldè
  Presidente del chapter italiano della
  Government Blockchain Association
  COO, Lynkeus Srl

- **SOFIE**, https://www.sofie-iot.eu/

  Contributor: Pritt Anton
  Program Manager and Business Analyst
  Guardtime

- PRIViLEDGE, https://priviledge-project.eu/

  Contributor: Sven Heiberg
  Product Manager
  Smartmatic-Cybernetica Centre of Excellence
  for Internet Voting

cyberwatching.eu consortium

Trust-IT Services
Communicating ICT to markets

Oxford e-Research Centre

UNIVERSITY OF OXFORD

ICT LEGAL CONSULTING
Balboni Bolognini & Partners

European Digital SME Alliance

CONCEPTIVITY
360 SECURITY

AON

aeiciberseguridad
Agrupación Empresarial Innovadora CIBERSEGURIDAD y Tecnologías Avanzadas

🔗 www.cyberwatching.eu

@cyberwatchingeu

/in/cyber-watching/

cyberwatching.eu has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 740129.