information

Review

Technologies of Data Protection and Institutional Decisions for Data Sovereignty

Enrico Del Re [1,2]

[1] Department of Information Engineering, University of Florence, 50139 Firenze, Italy; enrico.delre@unifi.it
[2] National Inter-University Consortium for Telecommunications (CNIT), Viale G.P. Usberti, 181/A Pal.3, 43124 Parma, Italy

Abstract: This paper aims to propose innovative actions of advanced technological solutions and consequent necessary institutional decisions to achieve in a reasonable time the definitive confidential data protection and data sovereignty, based on available scientific results. Confidential data protection is a fundamental and strategic issue in next-generation Internet systems to guarantee data sovereignty and the respect of human rights as stated in the foundation of the United Nations. Even if presently many international regulations are decisive steps to guarantee data protection within normative contexts, they are not adequate to face new technologies, such as facial recognition, automatic profiling, position tracking, biometric data, AI applications, and many others in the future, as they are implemented without any awareness by the interested subjects. Therefore, a new approach to data protection is mandatory based on innovative and disruptive technological solutions. A recent OECD report highlighted the need for the so-called Privacy-Enhancing Technologies (PETs) for the effective protection of confidential data, even more urgent for the coexistence of privacy and data sharing in international contexts. A common feature of these technologies is the use of software methodologies that can run on currently available microprocessors and their present immaturity. More effective and definitive protection can be achieved with another methodological approach based on the paradigm of '*Data Usage Control*'. This new concept guarantees data protection policy by default and initial design and it requires a new architecture of the data and a new HW&SW architecture of the computers. This contribution has a two-fold objective: first, to clarify why regulations alone and present technological proposals are not adequate for the effective and definitive protection of data and, second, to indicate the new necessary technological approach and the simultaneous institutional actions required to achieve the definitive protection and sovereignty of data in reasonable times, based on the results already available in the scientific literature.

Keywords: privacy and confidential data protection; data sovereignty; privacy-enhancing technologies; data usage control; technological solutions; fake data control; role of international institutions

Citation: Del Re, E. Technologies of Data Protection and Institutional Decisions for Data Sovereignty. *Information* **2024**, *15*, 444. https://doi.org/10.3390/info15080444

Academic Editor: Aneta Poniszewska-Maranda

Received: 11 June 2024
Revised: 26 July 2024
Accepted: 27 July 2024
Published: 30 July 2024

1. Introduction

Effective solutions for data protection are nowadays of paramount importance for the quality of daily life of people and the sustainability of the growth of the world economy, in particular in the present and future next-generation Internet (NGI) society.

Historically, the focus has been on the right to protect personal sensitive data (the so-called 'privacy'), which is stated in numerous international regulations. For example, Article 12 of the Universal Declaration of Human Rights (UDHR) of the United Nations (UN) for the first time in 1948 provided for this right, influencing the birth of subsequent legislative instruments, as the Charter of Rights of the European Union (Charter of Nice) proclaimed in 2000.

Since 2012 the European Union (EU) has tackled this problem and stated (referring specifically to the emerging framework of the Internet of Things, or IoT):

'Building trust in the online environment is key to economic development. Lack of trust makes consumers hesitate to buy online and adopt new services, including public e-government services. If not addressed, this lack of confidence will continue to slow down the development of innovative uses of new technologies, act as an obstacle to economic growth, and block the public sector from reaping the potential benefits of digitization of its services, e.g., in more efficient and less resource intensive provisions of services. This is why data protection plays a central role in the Digital Agenda for Europe, and more generally in the Europe 2020 Strategy' [1], and *'by design new systems must include as initial requirements:*

- *The right of deletion*
- *The right to be forgotten*
- *Data portability*
- *Privacy and data protection principles*
- *Taking into account two general principles:*
- *The IoT shall not violate human identity, human integrity, human rights, privacy or individual or public liberties*
- *Individuals shall remain in control of their personal data generated or processed within the IoT, except where this would conflict with the previous principle.'* [2]

According to these general and challenging statements, the EU issued the so-called General Data Protection Regulation (GDPR) that entered into force in all Member States on 25 May 2018 [3]. This complex regulatory document deals with all cybersecurity requirements related to personal sensitive data and, particularly, to the confidentiality and privacy of data anyhow referred to the owner (defined as the data subject in the GDPR terminology). In the following years, the principles and regulations of GDPR gained widespread attention and international acceptance by institutions and Internet actors outside the EU thanks to its much-advanced statements. Human society, at large, must be grateful to the EU that, despite the many heavy attempts to avoid any rule by the major Internet service providers and by some national governments, it has been the first political institution in the world to state a regulatory normative for the protection of the privacy of user data.

Nowadays, the concept of data protection is wider as it refers not only to the privacy of personal sensitive data but more importantly to the broad class of any kind of confidential data, such as those relevant to the economy, finance, health, personal and national security, infrastructure, professions, e-government, etc. This present concept of data protection is strictly related to the objective of data sovereignty: a fundamental requisite in present and future Internet scenarios to guarantee the inalienable human rights and the sustainable development of human society.

More recently the president of the European Commission Ursula von der Leyen declared in the 2020 speech on the State of the Union: '*Data sovereignty as self-determination of individuals and organizations (and states) on how to control their data*' is part of European digital sovereignty, referring then to '*a technology where we can control ourselves what data and how the data is used*'.

The awareness that data protection regulations alone are no longer sufficient to guarantee it and that new technologies are necessary for a more efficient and hopefully definitive solution to the problem is emerging in technological and institutional frameworks worldwide.

This paper aims to clarify why normative regulations are not sufficient and to present the new technological approaches proposed in international contexts. Section 2 recalls the present state-of-the-art of the privacy protection regulations and clarifies their limitations. Section 3 introduces the concept of confidential data protection that refers not only to personal sensitive data but also to the broader class of data to be anyhow protected. Section 4 summarizes the indications of the recent report by the Organisation for Economic Co-operation and Development (OECD) that identifies some privacy-enhancing technologies (PETs) able to address in the future the protection of data, outlining at the same time their potentialities and present immaturity. Section 5 introduces the required new paradigm of '*data usage control*' for data protection and the technological tools to achieve

it, to overcome the limits of the PET, and to propose a definitive solution to data protection that in addition can provide possible countermeasures against fake data. Section 6 clarifies what international objectives, challenges, and actions must accompany the new technologies and are required to obtain a future definitive solution of data protection and, finally, Section 7 concludes by outlining the realistic political and economic obstacles to the definitive solution of data protection together with the hope of overcoming them (as was carried out with the GDPR) for the benefit of the future digital human society.

2. State-of-the-Art of Privacy Protection Regulations

The basic principles and guidelines of GDPR, when someone or something is collecting, processing, and storing personal data, are lawfulness, fairness, transparency, minimization, purpose limitation, security, accuracy, and integrity. Another key and distinguishing feature is that the service providers must ask the data subject for consent defined as '*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*' ([3], preamble 32). Consent is not given once and forever, but must be renewed whenever personal data are used for purposes other than those initially authorized. Heavy penalties are imposed on service providers who do not comply with the GDPR rules. GDPR is a significant step forward for the security and privacy protection of data subjects, as demonstrated by the worldwide acceptance of its principles, which have gained consensus outside Europe (California, Japan, Brazil, Singapore, New Zeeland, and others) and, perhaps obtorto collo, have been suggested even by the CEOs of major social networks in public events sponsoring their adoption on a worldwide basis (e.g., Tim Cook, Apple, Cupertino, CA, USA, October 2018, and Mark Zuckerberg, Facebook, Cambridge, MA, USA, March 2019).

Despite its innovative and advanced regulations, GDPR has some limits to guaranteeing personal data security and privacy in the future Internet society:

- First, the implementation of data protection requirements, even after the GDPR, is entrusted to service providers that should ensure their fulfillment. Heavy fines for non-compliance should convince service providers to implement all necessary tools and actions, but we all know that too often this has not been and is not the case.
- Second, currently offered services, in addition to complying too slowly with the GDPR rules, often do not implement the required security and privacy constraints '*by initial design and by default*'.
- Third, the GDPR does not fully respect the EU-stated principle '*Individuals must retain control of their data generated or processed within the IoT*', if this principle is to be exercised a priori, in itinere and a posteriori. Apart from the initial request for consent, no control by the owner of the subsequent authorized or unauthorized use of her/his data is guaranteed.

In addition, more recent technologies like automatic profiling (i.e., profiling without any human intervention) of personal data, automatic facial recognition, in perspective the analysis of individual pheromones in the near future [4] and, absolutely surprisingly, even car tires equipped with pressure sensors connected to the Internet [5] are examples of the access, acquisition, and processing of personal data that could not be ruled by the GDPR. Even more dangerous, the massive collection of personal data for the training of artificial intelligence algorithms raises serious ethical, legal, and geopolitical questions. The transformation of data into commercial assets enriches a few actors, consolidates market oligopolies, increases geopolitical dependence, and violates human rights.

In general, the protection of personal data is more than privacy in the strict sense as it extends the protection of the individual beyond the sphere of private life and in particular in social relationships, thus guaranteeing self-determination and control over the circulation of one's data (expanding into the right to protection of personal identity). It is therefore a question of guaranteeing personal freedom as a fundamental right, not only as physical freedom but also against all illegitimate control and interference from others.

Based on this right, therefore, each individual must require that the personal data be collected and processed by third parties only in compliance with the rules and principles established by the interested data subject. In addition, the individual must have control over all information regarding their private life and at the same time must master the tools to protect this information.

As a final remark, the purpose and limit of GDPR are the regulation of the protection of personal data. GDPR does not deal with the broader context of the protection of any type of confidential data.

3. Confidential Data Protection

Confidential data are not only those that refer to sensitive personal data (i.e., those of so-called privacy) but to many other contexts of daily life and society as a whole: economy, finance, health, personal and national security, infrastructures, professions, e-government, etc. Their protection is an essential prerequisite for data sovereignty to guarantee a correct implementation of data-driven applications across different organizations. Everyone agrees that they must be protected and a growing number of people are increasingly convinced that the new information technologies, together with their great and useful advantages, pose serious risks to data sovereignty and confidentiality. This belief is often accompanied by the resignation of the inevitability of even unauthorized use of one's data by third parties offering services and by the forced acceptance of the use of personal data as the only way to access the offered services.

Present and future pervasive and ubiquitous networks (5G/6G and optical connections), artificial intelligence (AI), and the Internet of Things (IoT) are technologies that access and produce a huge amount of data (Big Data), making it possible to obtain, store, process, provide, and transmit volume of data, which may refer to confidential information that can be acquired even without the awareness of the interested subjects. More importantly, we must worry not only about the future but also (and above all!) about the present, as is the case of the apps on our smartphones that can track and profile our daily lives even without the awareness of the owner. The same can be said when we connect and use the most popular Internet browsers and email clients. In all these cases, it is possible and almost certain that our confidential data are used by third parties without our awareness and explicit authorization.

It is not visionary to imagine that the scenario of future Internet systems looks like an ever-present distributed and global computer dealing with confidential data without the awareness of their owners with the probable violation of data sovereignty, and suggests a future world much worse than the one of the famous *Big Brother* described in Orwell's *1984*, with the concrete risk of violation of the fundamental human rights and of people becoming the new future digital slaves of a few big players.

Of course, future technologies and services can provide breakthroughs and enormous benefits to society and the people (e.g., for e-health applications and services to disabled and elderly people, environmental control and security, smart energy production and utilization, smart mobility management, industry efficiency, smart cities, smart buildings, media and entertainment, e-government, etc.) and it is a vital interest of the entire human society to preserve the benefits while reducing to the minimum the associated risks of violation of data sovereignty.

The solution of confidential data protection cannot rely upon even more advanced regulations like GDPR. We need a different approach to the problem of preserving the sovereignty of confidential data. This new approach can only be technological. Indeed, recently (8 March 2023), an OECD report [6] recognized and highlighted the need for the so-called privacy-enhancing technologies (PETs) for the effective protection of confidential data, even more urgent for the coexistence of privacy and data sharing among international boundaries.

The following section gives an overview of the interesting PET proposals of the OECD report, outlining their potential and limitations.

4. Privacy-Enhancing Technologies (PETs)

In the OECD report, privacy-enhancing technologies (PETs) are understood as a set of digital technologies, approaches, and tools that permit the collection, processing, analysis, and sharing of information while protecting the confidentiality of data and, in some cases, also their integrity and availability in commercial applications. PET concepts are not new but the latest advances in connectivity and computation capacity have led to a fundamental shift in how data can be processed and shared. While still in their infancy, these developments hold immense potential to move society closer to the continuing process and practice of privacy by design, and thereby foster trust in data sharing and re-use. In particular, PETs enable a relatively high level of utility from data, while minimizing the need for data collection and processing.

The report also outlines that a growing number of policymakers and privacy enforcement authorities (PEAs) are considering how to incorporate PETs in their domestic privacy and data protection frameworks. However, the highly technical and fast-evolving nature of these technologies often presents a barrier to the understanding by organizations and to their consideration and implementation of policy and legal frameworks applicable to data. The high potential of PETs to protect the confidentiality of (personal and non-personal) data is recognized and this potential will help raise the level of privacy and data protection and promote the rights of individuals. However, apart from a still limited number of solid and convincing data processing use cases, there is also the awareness that the level of maturity of PETs is still unequal.

The report also states that while some of these technologies are not new, many are evolving and may ultimately warrant a reevaluation of regulations on data collection and processing. As a key challenge, these technologies often fall outside the radar of policymakers and regulators given their highly innovative nature and technical details that make them difficult to be understood and to evaluate their potential applications. These technologies are highly technical, creating a significant 'language barrier' between engineers building these systems and the policymakers and regulators who will ultimately determine how to use them. Therefore, these technologies with their different stages of development will likely need to be fully understood by institutional policy makers and to be part of broader political data governance frameworks. PETs cannot substitute legal frameworks but have to cooperate with them so that their applications need to be combined with legally binding and enforceable obligations to protect privacy and data protection rights.

The report recognizes that the concept of PETs is far from new; however, it has never reached a universally accepted definition. Over the years, different organizations have come up with their definitions of PETs and the categorizations of the corresponding technologies, extensively recalled in the document.

Therefore, the objective of the report is to propose a new agreed taxonomy for classifying PETs. The report identifies 14 different types of PETs that are classified into four broad categories:

- Data obfuscation
- Encrypted data processing
- Federated and distributed analytics
- Data accountability

The 14 PETs and their categorisation is reported in the following Table 1, extracted for clarity's sake directly from [6], together with potential applications, challenges, and limitations.

Let us briefly summarize the potential technologies and their limitations. For more comprehensive and complete information the reader can access directly the report [6].

Data obfuscation tools include zero-knowledge proofs (ZKPs), differential privacy, synthetic data, and anonymization and pseudonymization tools. These tools increase privacy protections by altering the data, by cryptography or by removing identifying details. Obfuscating data enables privacy-preserving machine learning and, in particular

ZPKs, allows information verification (e.g., age verification) without requiring sensitive data disclosure. However, data obfuscation tools can leak information if not implemented carefully. Anonymized data, for instance, can be re-identified with the help of data analytics and complementary data sets. Obfuscation measures including anonymization often involve complex processes that would need to be implemented by trained data scientists to ensure that no information is leaked unintentionally. Some technologies, such as ZKPs, have found niche uses in cryptocurrency applications, but there is significant room for further developments in different applications.

Table 1. Overview of major types of PETs, their opportunities and challenges.

Types of PETs	Key Technologies	Current and Potential Applications *	Challenges and Limitations
Data obfuscation tools	Anonymisation/ Pseudonymisation	Secure storage	- Ensuring that information does not leak (risk of re-identification) - Amplified bias in particular for synthetic data - Insufficient skills and competences
	Synthetic data	Privacy-preserving machine learning	
	Differential privacy	Expanding research opportunities	
	Zero-knowledge proofs	Verifying information without requiring disclosure (e.g., age verification)	- Applications are still in their early stages
Encrypted data processing tools	Homomorphic encryption	Computing on encrypted data within the same organisation Computing on private data that is too sensitive to disclose Contact tracing/discovery	- Data cleaning challenges - Ensuring that information does not leak - Higher computation costs
	Multi-party computation (including orivate set intersection)		
	Trusted execution environments	Computing using models that need to remain private	- Higher computation costs - Digital security challenges
Federated and distributed analytics	Federated learning	Privacy-preserving machine learning	- Reliable connectivity needed - Information on data models need to be made available to data processor
	Distributed analytics		
Data accountability tools	Accountable systems	Setting and enforcing rules regarding when data can be accessed Immutable tracking of data access by data controllers	- Narrow use cases and lack stand-alone applications - Configuration complexity - Privacy and data protection compliance risks where distributed ledger technologies are used - Digital security challenges - Not considered as PETs in the strict sense
	Threshold secret sharing		
	Personal data stores/Personal Information Management Systems	Providing data subjects control over their own data	

Note: (*) Only one application has been included for the sake of readability.

Encrypted data processing tools represent the most important step forward in confidential data processing among the PETs presented in the report. They include homomorphic encryption, multi-party computation including private set intersection, as well as trusted execution environments. Encrypted data processing PETs allow data to remain encrypted while in use, thus avoiding the need to decrypt the data before processing. For example, encrypted data processing tools were widely deployed in COVID tracing applications. Presently, they have limited applications and high computation costs, with emerging techniques to reduce this, and do not guarantee protection against digital security breaches.

Federated and distributed analytics allow the execution of analytical tasks (e.g., training models) upon data that are not visible or accessible to those executing the tasks. In this way, only the summary statistics or results are transferred to those executing the tasks. This allows sensitive data to remain under the custody of a data source while it is analyzed by

third parties. In federated learning, for example, data are pre-processed at the data source. In this way, only the summary statistics/results are transferred to those executing the tasks. Federated learning models are deployed at scale, for instance, in predictive text applications on mobile operating systems to avoid sending sensitive keystroke data back to the data controller. Federated and distributed analytics can still leak information, for instance, in the parameters sent back to the data controller. The use of federated and distributed analytics also relies on stable connectivity. This can be challenging for applications that require the continuous availability of analytic results.

Data accountability tools offer new controls over how data can be gathered and used or provide transparency and immutability into transactions. Data accountability tools include accountable systems, threshold secret sharing, and personal data stores. These tools seek to enhance privacy and data protection by enabling data subjects control over their data, and to set and enforce rules for when data can be accessed. Most tools are in their early stages of development, have narrow sets of use cases, lack stand-alone applications, and are barely ready for broad adoption (accountable systems and personal data stores). They give the responsibility for data protection to the storing and processing devices of data controllers that must be trusted.

As a conclusion, the report recognizes that, apart from a still limited number of data-processing use cases, there is also agreement that the present level of maturity of PETs is still unequal and in general PETs are not ready for wide applications and deserve further technological developments for effective protection of confidential data.

Another possible technological tool for data protection is the use of Blockchain, which the report mentions briefly. When applied to confidential data, Blockchain can track the use of the data in a trusted and unchangeable database. Therefore, the actual use, correct or not, of the data can only be verified *a posteriori* by accessing the trusted database of all performed data transactions. It can effectively be used to contest unauthorized use of the data but gives no control on *a priori* effective data protection.

As a final comment, all the mentioned technological tools rely on their trusted implementation by third parties, such as service providers, data controllers, data storage and processing actors, and similar. This is the main flaw of all these approaches, as they do not fulfill the EU-stated principle that '*Individuals must retain control of their personal data generated or processed within the IoT*', if this principle is to be exercised a priori, in itinere and a posteriori.

To achieve this objective, we need a new paradigm and new technological SW and HW tools for effective confidential data protection. The following section clarifies this new concept and the required technological approaches.

5. New Paradigm and Technological Tools for Data Protection

To avoid, perhaps and hopefully definitively, the violation of our fundamental rights, we need a new paradigm, not mentioned in the OECD report, for the sovereignty and the protection of confidential data. It is referred to in the literature with the term '*data usage control*', (most recent reference [7]), which can be defined as: '*except in cases of force majeure or emergency, any use in any form and for any purpose of confidential data must be previously and explicitly authorized by the owner for their correct use*' [8].

To achieve this highly challenging objective, we need to synergize the normative regulations, like GDPR, the new efficient technological tools specifically dealing with the direct control by the data subject of her/his data and political decisions.

First, let us consider the possible new technological tools. Avoiding the need to request every time authorization from the data owner, an advanced and innovative technological architecture is necessary for both data and computers, as will be clarified in the following based on research results and proposals already reported in the scientific literature.

5.1. Available SW Solution for 'Data Usage Control'

The new paradigm of confidential data protection ('*data usage control*') has been addressed in the scientific literature by innovative technological solutions that define a different structure of data and SW tools dealing with it.

The new structure of data is no longer a passive set of bits as it must incorporate a form of intelligence (metadata) that defines their '*usage policy*', to carry out authorization, control and self-defense action in any application context; the '*usage policy*' defines what can be done and what cannot be done with the data; the new structured data are properly encrypted.

Specific and innovative SW tools have been developed that access, decrypt, and process the structured data only in accordance with their '*usage policy*'. Any other kind of SW cannot decrypt the structured data. In that way, the confidentiality of data and their correct use are guaranteed.

For example, this approach is described in recent international scientific literature [9]. There are already partial experimental research implementations, in particular, e.g., by the Fraunhofer Institute in Germany in the context of the so-called International Data Spaces (IDS) [10,11], by the European Union DUCA project [12], and by the National Research Council in Italy [13,14].

All these implementations run on presently available microprocessors. Therefore, they represent affordable, effective, and usable SW solutions for the new paradigm of data protection.

May we be satisfied? Partially yes, as these technological solutions work well and could be widely employed in common applications and contexts. However, the SW tools for processing confidential structured data require significant computational resources, longer processing delays, and some breaches are always possible. In addition, in some cases, they rely again upon trusted third parties.

Hence, we must go further and look for an even more efficient and, in a certain sense, definitive solution to confidential data protection.

5.2. New HW&SW Computer Architecture for 'Data Usage Control'

It is time to rethink computer design from the foundations [15]. A new HW&SW architecture of computers can integrate and complete the previous structured-data SW architecture. The new HW&SW computer architecture, clearly described in very interesting papers [15,16], exploits the previously described new encrypted structured data.

The proposed innovative concept of HW&SW computer architecture is such that the new microprocessors and operating systems by default are designed to access, decrypt, and use the data according to their '*usage policy*'.

The basic concept of this new computer architecture processing confidential data is implemented according to Figure 1, directly from [15].

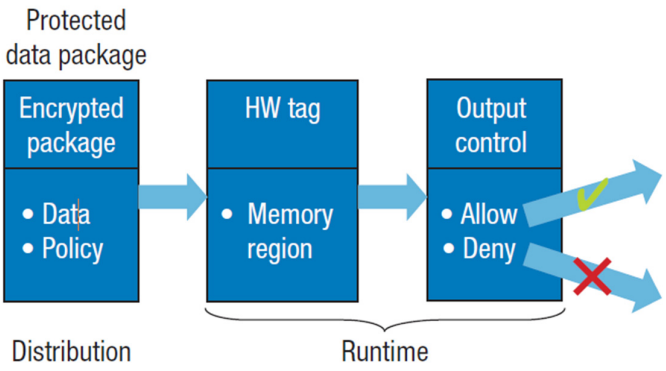

Figure 1. Basic concept for an HW&SW architecture designed to support data '*usage policy*' [15].

Computer SW translates the high-level '*usage policy*' into low-level HW tags. These are then associated with the memory locations where the decrypted data will be placed.

The tags are propagated along with the data as they are being processed. When any output is requested, the HW checks the tags to determine whether output for the data is allowed. This step prevents information from leaking out of the machine in which access has been given. When the app completes its operation on the data, any data that have been modified are re-encrypted and repackaged with their original '*usage policy*', before being written back to storage or transferred to another machine [15].

This computer implementation approach differs from typical software-only solutions in that it uses hardware to protect data according to their '*usage policy*', reduces computational burdens and processing times, and improves the overall system security.

Astonishingly although not unexpectedly, at present research and implementations of the proposed innovative HW&SW architecture of the computer systems processing the new encrypted structured data are missing, but together they would make sovereignty and protection of confidential data a much more effective and definitive solution.

5.3. New Architectures of Structured Data and Computers against Fake Data

The combination of the encrypted structured data and the new HW&SW computer architecture could be exploited to prevent the diffusion of fake data. Typically, fake data are characterized by the target of a wide audience, often through social networks.

In the new scenario implementing the concept of '*data usage control*', data will be of two types: conventional data (as they are now) or encrypted structured data.

Conventional data with the target of a wide audience, by default, could be suspected as 'fake' and therefore subject to worldwide warning. On the contrary, structured data with their '*usage policy*' of a wide audience could be more easily controlled, e.g., by the identification and trust of their source.

We have seen that only the encrypted structured data and the SW implementation of their correct use in present computers have been demonstrated and achieved, whereas the proposal of the new HW&SW computer architecture has not received the deserved attention and, until now, no specific actions have followed.

Now the time has come to promote the research for an effective implementation of this new computer architecture. This new HW&SW architecture must be pursued and can be obtained by a convincing and decisive research activity. In addition, it must be supported by consequent parallel international agreements and actions. Political and institutional decisions in favor of a wide and legally imposed implementation of this technological solution would take a decisive step forward for the protection and the sovereignty of data. The next section clarifies this requirement.

6. International Objectives and Challenges

What future actions are necessary? The technological solutions of data protection and sovereignty, even when achieved in their most advanced version, alone are not sufficient. The definitive fulfillment of the sovereignty and the protection of confidential data at least requires three necessary international steps and initiatives:

1. Consistent and constant funding of scientific and technological research to complete and integrate the new encrypted structured data and computer architecture to create efficient and effective tools for future Internet scenarios and at the same time simple enough for common use (based on the proposals already available in the literature). Responsibly keeping in mind that time is not an independent variable, the results must be obtained within a reasonable time before the sovereignty and the protection of confidential data will be definitively compromised by old and new supranational actors, not democratically controllable, that will be able to use the data obtained, more or less legally, for their power and market purposes.
2. Once obtained these new technological tools, it is mandatory to promote an international standardization of the new encrypted structured data and computer architecture.
3. To issue normative regulations to guarantee and certify that all future systems processing confidential data must comply with this standard requiring a quality marking,

as proposed, e.g., in the recent Cyber Resilience Act [17] for all digital products and services to be marketed in the European Union.

The consequent scientific, financial, and normative political actions must take into account that:

- SW solutions to confidential data protection are already available on current microprocessors, but the definitive effective solution must work on computers with the new HW&SW architecture.
- The semiconductor manufacturers (together with research centers) should be convinced to invest in the new HW&SW architecture by appropriate political actions that will identify the sovereignty and protection of confidential data as the indispensable mandatory objective of future Internet systems.
- The political institutions and the semiconductor manufacturers that pursue and obtain these objectives will achieve the great and unique opportunity to become the leaders in a new semiconductor technology of computing systems compliant with data protection and sovereignty, gaining a key competitive advantage in an extraordinarily large number of potential applications and to be the technological and regulatory creators of the new paradigm for the sovereignty of confidential data, thus being recognized with the status of benefactors of the future Internet society.

7. Conclusions

No doubt that the three steps outlined above are very challenging. Step 1 can be obtained in reasonable times by convincing sufficient and dedicated technological research. The most difficult ones are steps 2 and 3, as they involve political decisions that by their nature are difficult to agree upon and generally require longer times. However, they are necessary if we do not want the technological solutions, if and when achieved, to remain only a beautiful, interesting, original, remarkable scientific result without any application impact. Not doing this would be a missed opportunity for the protection of rights and the improvement of the quality of life in the future digital society.

No doubt that these steps will be faced against enormous supranational and government interests (as was the case for the GDPR). However, the future of democracy and the liberty of humanity require effective tools to preserve data protection and sovereignty.

The international institutions, although unfortunately currently focused on other priorities, should have the courage and foresight to support these technological and political initiatives for the definitive fulfillment of the sovereignty and protection of confidential data for the benefit of the whole future Internet society and the respect of the human rights as stated in the foundation of the United Nations.

The international scientific community has the great responsibility to support the implementation of these actions and to convince political decision-makers to act accordingly.

This is necessary if we want our future children and grandchildren to feel free world citizens and not slaves to uncontrollable and hidden actors.

This is a mandatory hope for the future!

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The author declares no conflict of interest.

References

1. European Commission, 25.01.2012, SEC(2012)72 Final, Page 7. Available online: https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf (accessed on 10 June 2024).
2. European Commission. IoT Privacy, Data Protection, Information Security. 2013. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed on 10 June 2024).
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46. *Off. J. Eur. Union (OJ)* **2016**, *59*, 1–88.
4. Privacy 2030: A New Vision for Europe. Available online: https://iapp.org/resources/article/privacy-2030/ (accessed on 10 June 2024).
5. Available online: https://on24static.akamaized.net/event/45/48/66/9/rt/1/documents/resourceList1712772467097/kb4surveillancewebinarslides1712772467097.pdf (accessed on 10 June 2024).
6. OECD. *Emerging Privacy-Enhancing Technologies: Current Regulatory and Policy Approaches*; OECD Digital Economy Papers, No. 351; OECD Publishing: Paris, France, 2023. [CrossRef]
7. Jung, C.; Dörr, J. Data Usage Control. In *Designing Data Spaces*; Otto, B., ten Hompel, M., Wrobel, S., Eds.; Springer: Cham, Switzerland, 2022. [CrossRef]
8. Del Re, E. Which future strategy and policies for privacy in 5G and beyond? In Proceedings of the 2020 IEEE 3rd 5G World Forum (5GWF), Bangalore, India, 10–12 September 2020; pp. 235–238. [CrossRef]
9. Munoz-Arcentales, A.; López-Pernas, S.; Pozo, A.; Alonso, Á.; Salvachúa, J.; Huecas, G. An architecture for providing data usage and access control in data sharing ecosystems. *Procedia Comput. Sci.* **2019**, *160*, 590–597. [CrossRef]
10. Available online: https://internationaldataspaces.org/data-sovereignty-updated-position-paper-on-data-usage-control-in-the-ids/ (accessed on 10 June 2024).
11. Otto, B. The Evolution of Data Spaces. In *Designing Data Spaces*; Otto, B., ten Hompel, M., Wrobel, S., Eds.; Springer: Cham, Switzerland, 2022. [CrossRef]
12. Available online: https://cordis.europa.eu/project/id/101086308 (accessed on 10 June 2024).
13. Lazouski, A.; Martinelli, F.; Mori, P. Usage control in computer security: A survey. *Comput. Sci. Rev.* **2010**, *4*, 81–99. [CrossRef]
14. Marra, A.L.; Martinelli, F.; Mori, P.; Saracino, A. A Distributed Usage Control Framework for Industrial Internet of Things. In *Security and Privacy Trends in the Industrial Internet of Things. Advanced Sciences and Technologies for Security Applications*; Alcaraz, C., Ed.; Springer: Cham, Switzerland, 2019. [CrossRef]
15. Lee, R.B. Rethinking computers for cybersecurity. *IEEE Comput.* **2015**, *48*, 16–25. [CrossRef]
16. IEEE Communications Magazine January 2017. Available online: https://www.comsoc.org/publications/magazines/ieee-communications-magazine/issue/ieee-communications-magazine-january-2017 (accessed on 10 June 2024).
17. Available online: https://www.european-cyber-resilience-act.com/ (accessed on 10 June 2024).