Telefónica Tech

Privacy and security implications of the convergence between IoT, Big Data and AI

Privacy and Security

telefonicatech.com

Telefónica Tech Cyber Security & Cloud's IoT and Smart Cities Cyber Security Innovation Centre

Privacy and security implications of the convergence between IoT, Big Data and AI

Privacy and Security

València, 2021

This joint project has been developed within the framework of Telefónica Tech Cyber Security & Cloud's IoT and Smart Cities Cyber Security Innovation Centre in Valencia, directed by **David Prieto Marqués.**

It was written by the team at Govertis Advisory Services, a Telefónica Tech company:

Coordinators:

Eduard Chaveli Donet, Head of Consulting Strategy

María Loza Corera, Lead Legal Advisor (New Challenges)

Joan Figueras Tugas, Lead Security & GRC Advisor

Authors:

Pablo Ballarin Usieto, Senior Advisor (Security & GRC)

Ángel Escudero Molina, Senior Advisor (Security & GRC)

Joan Figueras Tugas, Lead Advisor (Security & GRC)

María Loza Corera, Lead Legal Advisor (New Challenges)

Jordi Morera Torres, Lead Legal Advisor (Compliance)

Andreu Yakubuv-Trembach, Junior Advisor (Data Protection)

Vicente Segura Gualde, Head of IoT Security at Telefónica, and **David Prieto Marqués**, Head of Global Risk at Telefónica, participated in reviewing the project.

Technical data of the edition.

Index

Introduction.

The presence of products and services related to the IoT paradigm is already a reality. More than 30 trillion[1] IoT devices are expected to be connected by 2023, which is approximately three devices per capita. New IoT applications are emerging for practically every type of industry. The characteristics of 5G connectivity impact on the acceleration of the development of new functional capabilities on already known IoT applications such as: connected cars, virtual and augmented reality, wearables applied to fitness and e-health, or the family of 'smart' applications (Smart-City, Smart-Port, Smart-Village, Smart-Agro...), among many others.

In these examples, the contribution of three of the most relevant technologies of the last decade come to life: IoT, Big Data and Artificial Intelligence. Most IoT use cases would not be conceivable without the participation of the other two elements.

IoT is the main source of information. The thousands of connected devices generate millions of data. This data is optimised and analysed by Big Data technology. Machine Learning (ML) and Artificial Intelligence (AI) use the datasets to add value to the IoT services themselves or to other business areas of the IoT platforms, thus producing a virtuous circle between the three technologies.

This entire ecosystem, with its high degree of complexity, requires governance mechanisms that allow us to maintain control over devices, systems, processes and data, so that we can guarantee the correct functioning of each element from different points of view: ethical, legal, technical, economic, etc.

Like a conductor, Data Governance considers business, organisational and technical aspects equally and helps them work together to create a harmonious whole.

The benefits of digital transformation for society are largely based on the application of this technological trio to provide transformative solutions in every area of society: professional, business, personal, health, leisure, health care, etc...

However, this same potential has as a counterpoint the proliferation of new threats or the maximisation of some existing ones, which may affect people. Starting with the risks that may impact on the privacy and security of individuals whose data are collected and processed by these technologies according to business criteria that must be aligned with the need to preserve citizens' rights and freedoms.

In addition to regulatory compliance in both security and privacy, the ethical component must prevail in decision-making throughout the value chain of technology solutions and throughout their lifecycle.

[1] https://www.iotevolutionworld.com/iot/articles/446032-top-10-iot-use-cases.htm#:~:text=Another%20IoT%20use%20case%20is,are%20increasingly%20global%20and%20complex.&text=Low%2Dpower%20IoT%20devices%20are,to%20track%20shipping%20container%20openings

This publication is aimed at all those who may have some responsibility in the conception, design, implementation and exploitation of any technological solution based on any of these three technologies. The reader will find a compilation of the potential risks related to IoT, Big Data and Artificial Intelligence, catalogued in different areas such as ethics, legal, cyber security and privacy. The report provides an overview of the challenges posed by standardisation and presents the state of the art of the regulation that affects them and how Data Governance contributes to the achievement of the ethical, technical and cultural objectives set.

PART 1: Convergence between the three technologies

1. Basic elements and concepts.

BIG DATA

In information theory literature, data are understood as communication characters or symbols that can be formalised and reproduced (at will) and are easily transportable with the help of appropriate technical means. Data as such have no intrinsic meaning, they are "crude oil". But they can be carriers and/or facilitators of information, including coded information, acquiring particular meaning in a communication context (between people and/or between "things")[2].

Big Data is often characterised by the famous definition of the three 'V'[3]: **Volume**, **Variety** and **Velocity**. That is, handling a large volume of information (relative to the quantity), processing data at high speed or in real time (speed in obtaining interpretative results) and integrating a wide variety of information sources to, through different analytical techniques, generate knowledge and value. In addition, some authors and organisations have added further '**v**'s to define Big Data more precisely. For example, **Veracity** (the quality of the data captured is key), **Variability** (the meaning of the data changes frequently and inconsistencies can occur and need to be managed) and **Value** (the revenue or benefits of Big Data) which, on the other hand, have been criticised for being characteristics of the data itself rather than the concept of Big Data as such.

This macrodata concept, in addition to referring to the reality of massive data, points to the great opportunity that is offered once the technical capacity required for its analysis and use exists, allowing conclusions to be drawn quickly about the probability that certain events or patterns may occur. This is where Big Data can allow us to exploit our business more efficiently if we adopt a strategy with specific business objectives from the very beginning. However, implementing these and other innovative technological solutions in the interests of the business must respect legal and ethical limits, which we will discuss in later sections.

INTERNET OF THE THINGS (IoT)

The Internet of Things, also known as IoT, has been defined as "an infrastructure in which billions of sensors embedded in common, everyday devices ("objects" as such, or objects linked to other objects or individuals)

[2] HOFFMANN-RIEM, W., Big Data. Desafíos también para el Derecho, Pamplona: Civitas, 2018, pág. 51.

[3] LANEY, D., "3D Data Management: Controlling Data Volume, Velocity, and Variety", Application Delivery Strategies, META Group Inc, fichero 949, 6 de febrero de 2001, https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

record, process, store and transfer data that, when associated with unique identifiers, interact with other devices or systems using their networking capabilities"[4].

The development over the last two decades of the Internet of Things has been essential in shaping the surrounding environment of technological progress. The current state of a global Internet means that since 2016, the number of connected objects far exceeds the number of inhabitants. The billions of everyday objects interconnected in the network have three main sources of data: those provided voluntarily by the user, those perceived from the environment (location, speed, temperature, blood pressure, image, sound, etc.) and those generated by the device as it operates.

The IoT structure overcomes the barrier between objects in the physical world and with this, it is possible to move from the existence of traditional objects (considered passive) to intelligent objects (active), collecting information and transforming it into data that will later be processed and sent to the Internet. IoT fulfils the objective of optimising resources, that is, to make us capable of monitoring, counting and locating everything related to our "things", our productive factors and ourselves, greatly reducing expenses, losses and costs, as well as knowing in detail about the state of everything.

In fact, it makes more sense to shift to the new term 'Internet of Everything', which encompasses what we understand as the Internet of Things and its sectoral variant 'Internet of Robotic Things' (IoRT), broadening the scope to the reality of networking things, living things, their processes and data, all with greater technical capability, smart application and automation, while taking on a new dimension in human-to-human communication (H2H)[5].

ARTIFICIAL INTELLIGENCE (IA)

The human tendency to create its own replicas for tasks that require an exercise of intelligence is quite old and there are many historical aspects to the conceptualisation of Artificial Intelligence (AI). Notwithstanding the above, there is no unanimous or generally accepted concept of AI. In fact, there is no univocal conception of AI.

The European Commission understands that "the term artificial intelligence applies to systems that evidence intelligent behaviour, as they are able to analyse their environment and take action - with a certain degree of autonomy - in order to achieve specific objectives"[6].

---

[4] GT29, Dictamen 8/2014 sobre la evolución reciente del Internet de los Objetos, elaborado por el Grupo de Trabajo sobre protección de datos del artículo 29 (Unión Europea), 16 septiembre de 2014, pág. 4. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_es.pdf

[5] KALYANI, V.L., SHRAMA., D., "IoT: Machine to Machine (M2M), Device to Device (D2D) Internet of Everything (IoE) and Human to Human (H2H): Future of Communication", JMEIT, v. 2, nº. 6, diciembre de 2015,

http://www.jmeit.com/JMEIT%20Vol%202%20Issue%206%20Dec%202015/JMEITDEC0206003.pdf

[6] COMISIÓN EUROPEA, "Inteligencia artificial para Europa", Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones, COM(2018) 237 final, 25 de abril de 2018. https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-237-F1-ES-MAIN-PART-1.PDF

The European Commission's Independent High Level Expert Group on Artificial Intelligence (AI-HLEG) has since gone further by conceptualising Artificial Intelligence (AI) systems as human-designed software (and possibly also hardware) systems that, given a complex goal, act in the physical or digital dimension by perceiving their environment, acquiring data, interpreting the structured or unstructured data collected, reasoning about knowledge, or processing the information derived from this data and deciding on the best action(s) to take to achieve the objective set. As they point out, "AI systems can use symbolic rules or learn a numerical model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions"[7].

Meanwhile, the European Commission's Joint Research Centre points out four characteristics that are evident when talking about Artificial Intelligence [8]:

- perception of the environment and the complexity of the real world.
- information management (collection and interpretation of input data).
- decision making which includes aspects such as reasoning, learning and taking action.
- achieving predefined objectives.

In the Proposal for a European Regulation on Artificial Intelligence[9] the definition given to define an AI system includes the following characteristics: *"software that is developed with one or more of the techniques and approaches (...) and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with"*.

In turn, there are different types or categories of AI depending on their scope and field of application. We can speak of two types of AI: the so-called **weak** or **narrow AI**, which would be one that is specific or specialised in a certain task (for example, a virtual assistant such as Siri or Cortana); and the **strong AI**, which would be capable of approaching the AI's objective, carrying out activities as if it were a human. It differs from the former in that it has its own initiative. There is also talk of a **'super artificial intelligence'**, in the sense of one that will become equal to or greater than human intelligence.

Likewise, the AEPD also distinguishes between three types of Artificial Intelligence, but with other terms[10]: strong, general and weak AI, with general AI being that one which could solve any intellectual task solvable by a human being and would therefore be equivalent to that previously conceptualised as strong; while strong

[7] COMISIÓN EUROPEA, A Definition of AI: Main capabilities and disciplines, por el grupo de expertos de alto nivel en Inteligencia Artificial, 2018, pág. 6. https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

[8] SAMOILI, S., LÓPEZ COBO, M., GÓMEZ, E., DE PRATO, G., MARTÍNEZ-PLUMED, F., & DELIPETREV, B., AI Watch. Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence, Luxembourg: Publications Office of the European Union, 2020, pág. 8. https://ec.europa.eu/jrc/en/publication/ai-watch-defining-artificial-intelligence

N.B.: En dicho informe técnico, se parte de un análisis de 29 políticas e informes institucionales (por ejemplo, intentos de estandarización o estrategias nacionales), 23 publicaciones de investigación y 3 informes de mercado, desde 1955 hasta la fecha de publicación del informe.

[9] Artículo 3 (1), Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM (2021) 206 final. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=ES

[10] AEPD, Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción, 2020, p. 5. https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

AI would be equivalent to that previously mentioned as superintelligence, which would go beyond human capabilities.

Categorías de IA	*Categorías de IA según la AEPD*
Débil (estrecha)	Débil
Fuerte	General
Superinteligencia	Fuerte

Table: Correspondence between AI categories according to different bibliographical sources.

It is at this point where **algorithms**, as we call the ordered set of systematic operations that allow to make a calculation and find the solution to a type of problem, become vitally important. For our purposes, algorithms are parts of complex digital decision-making systems, composed of software and hardware, and integrated in socio-technological information systems.

There are different techniques depending on the progress made[11]. Thus, Machine Learning (ML) or **automatic learning**, involves giving the computer the ability to improve or learn by itself, without having to be explicitly programmed to do so. As stated by the AEPD "machine learning is related to data mining, optimisation and big data techniques" [12].

Deep Learning (DL) is a branch of ML, as both are machine learning techniques, but with the difference that DL is based on neural networks or layered data processing, trying to emulate the functioning of the human brain. In recent years, DL has brought about a huge revolution thanks to the greater cheapness and accessibility of specific hardware (GPUs / TPUs), which allows highly complex algorithms to be processed in a very short period of time. Another advantage of DL over traditional machine learning techniques is what is known as Representation Learning, or the ability to extract the intrinsic characteristics of data automatically. Thanks to DL, artificial intelligence fields such as Computer Vision and Natural Language Processing (NLP) have been boosted, helping to build solutions that nowadays coexist with people through our personal computers or mobile devices.

Therefore, we could define AI as that ecosystem where we find different technologies (ML, DL, etc.) which share the processing of data to obtain value and knowledge based on predetermined objectives. This is why

[11] LOZA CORERA, M., Op. Cit.

[12] AEPD, Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial..., Op.Cit.

we find definitions according to which "artificial intelligence is at the centre of all these solutions, at the point where everything converges"[13].

2. Convergence of the three technologies.

Today, every digital connection becomes a source of data, opening up - with its massification - a horizon of details that we were never able to see when we were limited to the smallest quantities[14]. In the new informational and communicational paradigm we live in, data are the cornerstone of the society of knowledge, something that in the productive aspect is reflected in the Fourth Industrial Revolution or Industry 4.0. In fact, the data economy is growing to such an extent that in the European Union, the monetisation of data could double its value in the next five years following 2020[15].

Big Data has burst into our society thanks to the combination of three key factors[16]. Firstly, the human factor, comprising both the people trained to decide and manage the algorithms (data scientists) and people who are dedicated to studying the business sector in order to implement the Big Data project. Secondly, we would find the technological resources (hardware and software) and finally, the data sources, which have previously unseen capabilities.

To analyse these immense amounts of data, a set of techniques have emerged that belong to the field of AI and are known as "data mining"[17]. This is why, closely linked to the concept of Big Data, we find that of Artificial Intelligence (AI), which feeds on and needs large amounts of data and makes it possible to exploit this big data. Thus, Artificial Intelligence is configured as a new factor of production and not as a mere driver of productivity[18], which would mean a real transformation of the existing panorama so far.

Two factors have been crucial to the development of AI: unlimited access to processing power and the growth of Big Data. We could say that "data is to AI what food is to humans" [19]. And that "food", understood as Big Data, is largely thanks to IoT, which can be considered as the "zero kilometre" of this huge data generation.

[13] LUCA, "¿Qué es la Inteligencia Artificial?", Diccionario Tecnológico. https://luca-d3.com/es/data-speaks/diccionario-tecnologico/inteligencia-artificial

[14] MAYER-SCHÖNBERGER, V., CUKIER, K., *Big data. La revolución de los datos masivos*, Madrid: Turner, 2013, pág. 22.

[15] IMREI, K. (Ed.), "Data as the Engine of Europe's Digital Future", *The European Data Market* Monitoring Tool Report, junio de 2019, pág. 53 http://datalandscape.eu/sites/default/files/report/EDM_D2.5_Second_Report_on_Policy_Conclusions_final_13.06.2019.pdf

[16] PÉREZ, C., "Aspectos legales del Big Data", *Revista de Estadística y Sociedad*, nº 68, 2016, p. 18.

[17] BARRIO, M. *op. cit.,* p. 42.

[18] PURDY. M, DAUGHERTY, P., Informe "Inteligencia Artificial, el futuro del crecimiento", Accenture, 2016, p. 4. https://www.accenture.com/cl-es/insight-artificial-intelligence-future-growth

[19] PURDY. M, DAUGHERTY, P., *Op. Cit.*, pág. 11.

This in retrospect: the enormous accumulation of information and Big Data is what has allowed the development of AI to become effective in recent years[20].

Another distinctive feature of AI would be its self-learning capability, which would set it apart from the technological advances of the past[21]. This is where the aforementioned concepts of Machine Learning and Deep Learning come into play, which precisely differentiate these systems from less advanced ones[22]. In this sense, AI has the capacity to overcome the physical limitations of capital and labour to open up new sources of value and growth.

We see, therefore, how the Internet of Things, Big Data and Artificial Intelligence - among other key agents of the new industrial revolution, such as robotics, 3D and 4D printing, nanotechnology, biotechnology and materials science, among others - are **realities that can hardly be understood separately**. In fact, thanks to IoT we feed Big Data processes, whose solutions are developed and reach their maximum potential with AI.

Furthermore, the convergence of the three technologies covers related approaches and techniques such as reinforcement learning, a specific example of Machine Learning; machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search and optimisation) and the whole of robotics, which includes control, perception, sensors and actuators, as well as the integration of all other techniques in cyber-physical systems.

Having established the indivisible relationship between Artificial Intelligence, Big Data and IoT, some authors point to a new technology that is part of this equation: Blockchain, which provides a secure exchange of information between entities in a distributed network and, it is claimed that it would mean an expansion of the Big Data concept in terms of the visibility of data transactions between all those involved.

In this context, the European Union has been very aware from the very beginning of the importance of data, and in particular, of the data economy, as in 2014 it approved the *Communication Towards a Thriving Data Economy*[23], to establish the appropriate framework conditions for a single market for Big Data and Cloud Computing, seeking to establish the characteristics of the future data economy. In this line, the European Commission has promoted the so-called data economy, in the context of the **Digital Single Market**[24], in the context of the Digital Single Market, whose strategy and roadmap were presented in May 2015, through the

[20] COTINO HUESO, L., "Riesgos e impactos del Big Data, la Inteligencia Artificial y la robótica. Enfoques, modelos y principios de la respuesta del Derecho", *Revista General de Derecho Administrativo*, nº50, 2019, p.7.

[21] CESE, "Inteligencia artificial: anticipar su impacto en el trabajo para garantizar una transición justa", Dictamen 2018/C 440/0, Comité Económico y Social Europeo, 6 de diciembre de 2018, p. 3.

[22] BEJERANO, P., "Diferencias entre machine learning y deep learning", Telefónica Think Big Empresas, 8 de febrero de 2017, https://blogthinkbig.com/diferencias-entre-machine-learning-y-deep-learning

[23] COMISIÓN EUROPEA, "Hacia una economía de los datos próspera", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM/2014/0442 final, 2 de julio de 2014, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52014DC0442&from=ES

[24] PARLAMENTO EUROPEO, "El mercado único digital omnipresente", Fichas temáticas sobre la Unión Europea Parlamento Europeo, https://www.europarl.europa.eu/factsheets/es/sheet/43/el-mercado-unico-digital-omnipresente

Communication, *A Strategy for Europe's Digital Single Market*[25]. This was followed in 2018 by the European Commission's presentation of an *Artificial Intelligence Strategy for Europe*[26], in the framework of which the White Paper on Artificial Intelligence[27] and the Communication *A European Data Strategy*[28] have been adopted where the Commission states that "data is an essential resource for economic growth, competitiveness, innovation, job creation and social progress in general". In June 2020, the Commission adopted a new Communication *Europe's time: repairing the damage and preparing the future for the next generation*[29] in which the Digital Single Market is identified as a key building block in respect of the recovery around COVID 19.

Here we should mention the Proposal for a European Regulation on European data governance[30] which aims to extend the availability of data for use, by increasing trust in data intermediaries and strengthening mechanisms for data exchange across the EU.

3. Current use of the three technologies.

What all three technologies have in common is that they are forward-looking and have infinite possibilities for application in all areas of our lives.

The following use cases in which they are currently being developed, both in the private and public sector, are worth mentioning:

- **Automation and sensorisation of homes (domotics), buildings and cities**, to achieve greater possibilities, physical experiences, satisfaction and monitoring of processes. When sensorisation is applied to the infrastructure of urban centres to achieve efficiency, we are speaking of **Smart Cities**.
- **Mobility, transport, intelligent vehicles in general and, in particular, autonomous cars**, the latter being, according to the DGT, all those "with motor capacity equipped with technology that

[25] COMISIÓN EUROPEA, "Una Estrategia para el Mercado Único Digital de Europa", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM(2015) 192 final, 6 de mayo de 2015, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52015DC0192&from=ES

[26] COMISIÓN EUROPEA, "Inteligencia artificial para Europa", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM(2018) 237 final, 25 de abril de 2018, https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-237-F1-ES-MAIN-PART-1.PDF

[27] COMISIÓN EUROPEA, *Libro Blanco sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza*, COM(2020) 65 final, 19 de febrero de 2020, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf

[28] COMISIÓN EUROPEA, "Una Estrategia Europea de Datos", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM(2020) 66 final, 19 de febrero de 2020, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0066&from=ES

[29] COMISIÓN EUROPEA , *"El momento de Europa: reparar los daños y preparar el futuro para la próxima generación"*, Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM(2020) 456 final,

https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2020/0456/COM_COM(2020)0456_ES.pdf

[30] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos), COM(2020) 767 final https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020PC0767&from=EN

allows them to be managed or driven without requiring the active control or supervision of a driver, whether this autonomous technology is activated or deactivated permanently or temporarily"[31].

- **Drones** which are defined as "any aircraft operated or designed to be operated without a pilot on board"[32].
- **Sensorisation in industrial manufacturing, commerce and consumption processes (B2B, M2M)** by connecting machines, parts and systems creating intelligent networks that can control each other and in an autonomous way. This is achieved through cyber-physical systems and the so-called internet of services[33].
- **Sensorisation of wearable devices**, the set of electronic devices that we wear as accessories, including those that are used through applications for health indications. It is especially in the health sector where Big Data and AI techniques are of particular relevance.
- **Fraud prevention and money laundering**

The transformative power of these technologies in improving our lives is evident from the very broad spectrum of application, and other systematic categories such as quality education, as well as digital transformation, climate change, sustainable development and cyber security.

According to an IoT-Analytics report[34] the platform market is concentrated in a few suppliers (generic platforms), but at the same time, it tends to fragment (specialised platforms) and is constantly growing.

Within this market, according to the IoT-Analytics report, there were 620 suppliers in 2019, an increase of a 37% compared to the number of suppliers in 2016, which was 260.

Following the aforementioned report, if we analyse these suppliers by sector, we find that the manufacturing and industry sector occupies 50%, well ahead of sectors like Energy (34%), Mobility (32%) and Smart Cities (31%). This is followed by areas such as healthcare, supply chain and retail, with agriculture (13%) almost on par with public administration (12%).

[31] DGT, "Instrucción 15/V-113 sobre autorización de pruebas o ensayos de investigación realizados con vehículos de conducción automatizada en vías abiertas al tráfico en general", Dirección General de Tráfico del Ministerio del Interior, p. 1, http://www.dgt.es/Galerias/seguridad-vial/normativa-legislacion/otras-normas/modificaciones/15.V-113-Vehiculos-Conduccion-automatizada.pdf

[32] COMISIÓN EUROPEA, Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de Seguridad Aérea de la Unión Europea, y se deroga el Reglamento (CE) nº 216/2008 del Parlamento Europeo y del Consejo, 2015/0277/COD, 7 de diciembre de 2015, artículo 3 (29).

[33] CEPAL, Informe "La Nueva Revolución Digital: de la Internet del consumo a la Internet de la producción". Comisión Económica para América Latina y el Caribe, 2018, p. 36, https://repositorio.cepal.org/bitstream/handle/11362/38604/4/S1600780_es.pdf

[34] IoT ANALYTICS, IoT Platforms Company Landscape 2020, https://iot-analytics.com/product/iot-platforms-landscape-database-2020

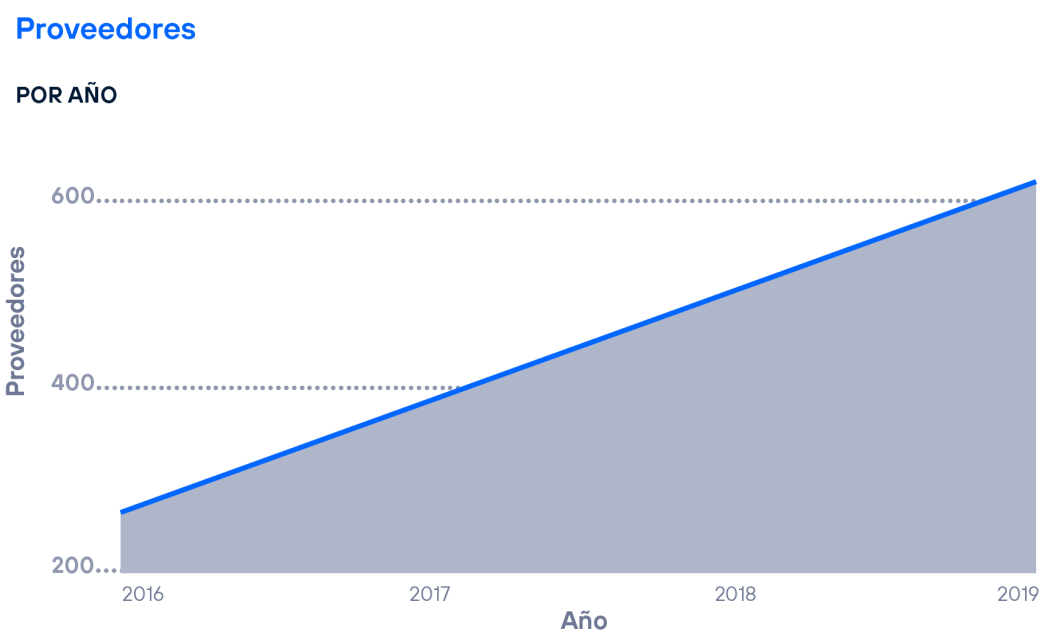


Figure 2: Evolution of suppliers by year. Own elaboration.

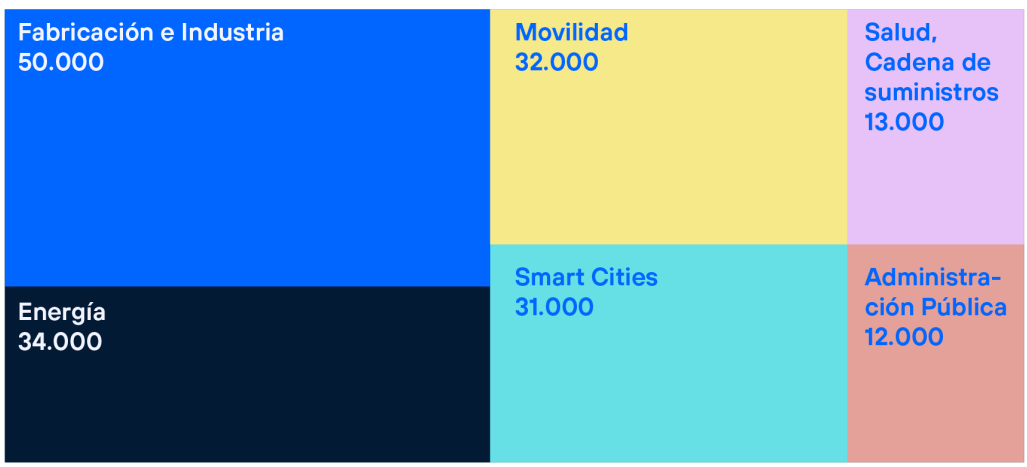
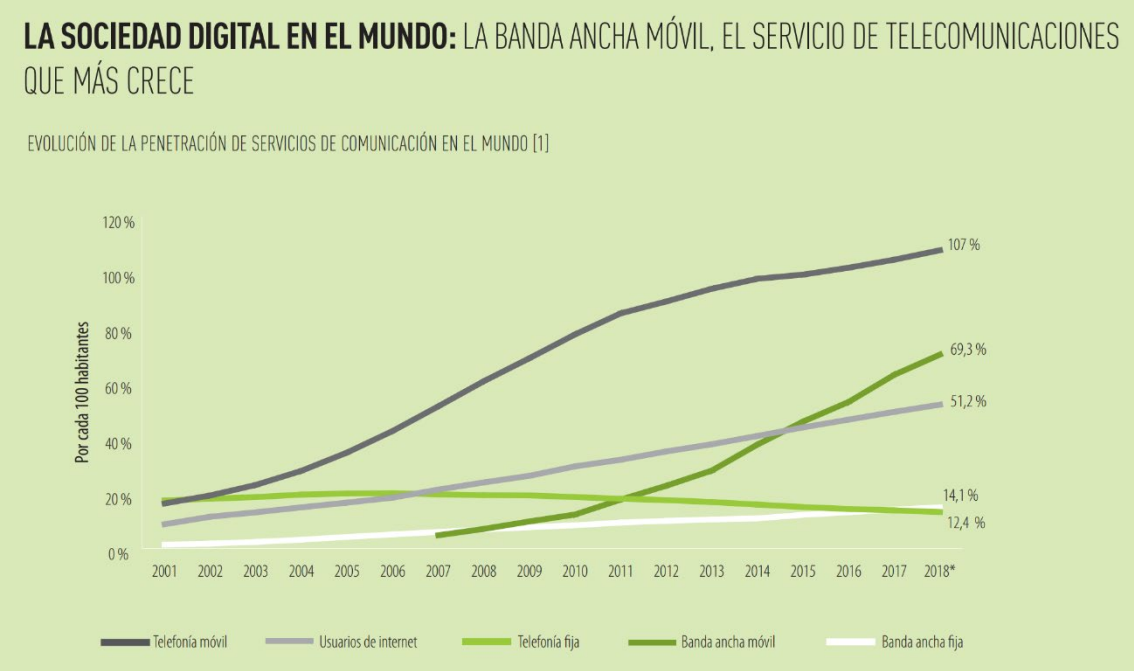


Figure 3: Suppliers by sector. Own elaboration.

If we look at the level of digitalisation, as a prior step for the existence and operation of these technologies in people's daily lives, according to the *Fundación Telefónica*[35], report, mobile broadband has undergone significant development in recent years, and regarding fixed broadband, more than half of subscriptions are made by cable or optical fibre. To be more precise, in Spain, the percentage of optical fibre lines exceeds 50%. The report[36] highlights that Spain, with respect to the connectivity indicator, "is the country with the best performance among the five main economies of the European Union".



Therefore, we see that in Spain we have the perfect substrate for the implementation and development of these technologies. According to the consultancy company IDC[37], Spain is the fifth country in Europe in terms of investment in IoT, only behind Germany, the United Kingdom, France and Italy.

[35] RODRÍGUEZ CANFRANC, P. et al., "Sociedad Digital en España 2019", Fundación Telefónica, abril 2020, pág. 28, https://www.fundaciontelefonica.com/noticias/informe-sociedad-digital-espana-2019

[36] Ibidem, pág. 29.

[37] IDC RESEARCH ESPAÑA, "El Mercado de Internet de las Cosas en España", https://idcspain.com/research/IoTSpain

4. Data Governance (DG)

Data Governance is defined as the set of roles and policies that are used for the correct management of data within a company, country, nation, community, from the definition of the source systems, through the business processes, technical processes, to the security and exploitation of said data.

The European Union, as the first of the measures announced in the framework of the 2020 European Data Strategy[38], has presented a proposal for a European Regulation on data governance ("Data Governance Act"[39]) which aims to create a common European data space by establishing the necessary conditions for the sharing of data in the internal market, through the creation of a harmonised framework for its exchange and thus favouring and promoting the data economy. Hence, we can see the importance of data governance also for compliance purposes, but which ultimately and for any organisation will allow an adequate, efficient, secure and compliant management of the different existing regulatory frameworks affecting data (personal and non-personal).

Data has been referred to as "the food of AI". Data Governance ensures the quality of this food, as well as guaranteeing the origin and destination of the data (who produces it, who consumes it, what processes it undergoes) and is also the technical vehicle on which the legal regulation of data access is implemented.

Data processing systems have traditionally implemented different technical control mechanisms, operating independently of one another. The contribution of Data Governance is **to orchestrate** these and other mechanisms to achieve **a holistic approach to the solution**, encompassing not only the **technical** part but also the organisational and **business part**.

New technologies such as 5G, Big Data or IoT, focused, for example, on infrastructure management (Smart Cities), highlight the immense amounts of current and future data.

The European Union indicates that data growth from 2018 to 2025 is expected to **increase by a 530%** (see European Data Strategy[40]). This exponential growth of data must be governed to ensure the ethics, quality, security and many other aspects of this "digital twin".

A concept in vogue right now is that of the **digital twin**. It refers to the replication of everyday life in information systems and applies to both industrial processes and individuals. This opens up the need for strong Data Governance mechanisms to ensure that concepts such as ethics, fairness and security are applied to these twins, since they impact on the real world.

While an industrial process can benefit greatly from these models, in their application to individuals, caution and care must be exercised, given the sensitive nature of the data being processed.

Another of today's hot topics are **data trusts or cooperatives**, linked to **shared data spaces** (as opposed to silos or duplicate data). These spaces use a series of contracts between parties whereby

---

[38] COMISIÓN EUROPEA, "Una Estrategia Europea de Datos", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM(2020) 66 final, 19 de febrero de 2020, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0066&from=ES

[39] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos, (Ley de Gobernanza de datos), COM(2020) 767 final https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020PC0767&from=EN

[40] EUROPEAN UNION: Data Governance in Data Strategy. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

data subjects altruistically give up their data to be processed for defined purposes by other entities (beneficiaries) while retaining control over the data they generate. Implicit in this concept is strong security, privacy and regulatory management, in short, effective governance of that data.

These trusts or cooperatives are sometimes run in the form of a data marketplace with contracts implemented and secured with **Blockchain**, which guarantees the traceability and uniqueness of the data.

The European Union in its European Data Strategy [41] speaks about the need for these common spaces concerning:

- industry (manufacturing)
- European Green Deal
- mobility
- health
- finances
- energy
- agriculture
- public administrations
- in the field of qualifications

These spaces must be careful to avoid bias and opacity, and guarantee rights and freedoms, as well as optimise designs, all with a view to improving efficiencies and benefits.

On common spaces it is important to apply the principle: "Data as open as possible, as secure as necessary". **FAIR** principles for sharing and democratisation of data:

F- Findable

A- Accessible

I- Interoperable

R- Reusable

At a national level, the entire European strategy and law on data governance is capillarised in different actions and levers set out in the BOE (Spain´s Official State Bulletin)[42], such as Agenda España Puede[43], ENIA[44], etc.

We would like to mention in this section one of the fundamental pillars on which Data Governance is based and which enables the correct management of information: metadata.

[41] Op. Cit.

[42] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-10008

[43] https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/230720-Espa%C3%B1aDigital_2025.pdf

[44] https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIAResumen2B.pdf

Metadata is contextual information that accompanies data and allows the application of different disciplines such as quality, security, organisation, legal aspects, life cycle, data source integration.... closely related to ensuring the rights of both natural and legal person.

PART 2: Ethical impact

The set of emerging technologies explored in this study, and in particular Artificial Intelligence, opens the door to new ethical issues, and it is therefore necessary to consider the impact of the possible consequences on the lives of people who may be affected by these technologies. These consequences have not been present until now, or to be more precise, have not been present with the same intensity. We are talking about systems that can increase social inequalities, make mistakes in systems that are vital for people (justice, human resources), encourage harmful consumer behaviour, etc., and we must work to ensure that this does not happen.

It is therefore essential to identify these problems and understand the way in which they are being dealt with by different organisations and companies. The aim is to build systems based on Artificial Intelligence in accordance with ethical guidelines for the common good of humanity and not just for functionalities or business objectives.

BIASES

The consideration of biases as one of the main risks of AI is common in those studies or reports that particularly focus on the ethical and legal dimension of such technology. However, as we will see, the different ways in which biases originate mean that they need to be addressed not only in the field of AI, but also in IoT devices and in the context of Big Data.

In its report on Artificial Intelligence[45], he Catalan Data Protection Authority mentions the classification of different types of bias carried out by BAEZA-YATES, Professor of Computer Science at Pompeu Fabra University and Northeastern University, who classifies three types of classic biases: statistical, cultural and cognitive.

Broadly speaking, statistical bias, according to the above classification, comes from the way in which we obtain the data, for example, through measurement errors in this first phase of obtaining information. It is clear that much of the risk in the correlation of IoT devices, Big Data systems and AI, would fall on the former, since possible errors in obtaining information from the IoT device could generate this statistical bias with the corresponding impact on the subsequent information processing process. Cultural bias is based on group conceptions as a society, for example, stereotypes that may exist about a certain group of people based on their nationality, gender, religion or social status. Such biases have a direct impact on the results produced by artificial intelligence systems, causing decision-making to increase inequality among minority or disadvantaged groups. Inaction in the face of such problems in AI could mean that new data generated by these systems will continue to suffer from these discriminatory problems, creating a negative feedback loop

[45] APDCAT, *Inteligencia Artificial:* Decisiones Automatizadas en Cataluña, 2020, pág. 21, https://apdcat.gencat.cat/web/.content/04-actualitat/noticies/documents/Informe-IA-Castellano.pdf

that will cause the problem to persist in society. Finally, can find the cognitive biases, already linked to the individual level, which will depend on the individual's own preferences, convictions, etc. This last bias can be especially useful, once an individual has been profiled, to provide them with information designed to please them in order to reaffirm their own convictions and, if necessary, even to provide or generate fake news for this purpose, to keep them in a sort of filtered bubble.

The materialisation of such risks can have fatal impacts on users and citizens and would be a "technological wash" that would make people believe that algorithmic decisions are fair when in fact they are reproducing a bias among society[46].

OPACITY

This is a risk that, although it affects all information systems across the board, may be especially relevant in the context of these new technologies. The GDPR places the principle of transparency[47], as one of its pillars, being perhaps one of the aspects that can be most easily assessed by data subjects today: am I being correctly informed about the purposes or legal bases when I submit my CV to a job portal? Does this application correctly inform me about exactly what data it uses about me to carry out its functions?

This principle becomes even more relevant and even more complex when our data are processed to generate automated decisions about us, and even more so if such decisions may have important consequences on our rights and freedoms. This issue does not go unnoticed by the European legislator, when referring to automated decisions, in its Recital 71[48], when it speaks of the principles of fairness and transparency, and which it also places as an aspect that must be informed to data subjects in compliance with Articles 13 and

[46] RICHARDSON, R., SCHULTZ, J., CRAWFORD, K., "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice," *94 N.Y.U. L. Rev. Online,* nº 192, marzo 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333423

[47] ***N.B.:*** *Artículo 5 (Principios relativos al tratamiento) del RGPD: "1. Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»)"; Considerando (39): "...El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con el tratamiento."*

[48] ***N.B.:*** *Considerando 71 del RGPD: "A fin de garantizar un tratamiento leal y transparente respecto del interesado, teniendo en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado y se impidan, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto. Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas".*

14[49]. This information refers at least to "*...meaningful information on the logic applied and the significance and expected consequences of the processing for the data subject...*"[50].

However, the generality of the term used to define the obligation to inform about this automated processing may raise legal questions about the scope of other interests involved, since fully detailed information about the process of the algorithm or logic applied by an AI system on a decision, assuming that it could be transferred in a way that is understandable to the average citizen, could be revealing trade secrets or even know-how processes susceptible to legal protection, patents or intellectual property if applicable, jeopardising all or part of the business model or strategies of the different economic operators. On the other hand, information that is too generic may distort the very principle of transparency and not provide any information to the citizen, contributing to what is known as the "black box" effect in the AI context.

The aforementioned black box effect is used by the European Commission, in its "Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and Robotics"[51], to illustrate the potential risks, especially in terms of liability, when we integrate AI with other devices, such as IoT devices, and we do not have enough information about how the system interacts until the final decision is made.

RIGHTS AND FREEDOMS

It is therefore not surprising that, as a result of these biases, the statistical, cultural and cognitive errors that may affect the three aforementioned technologies, together with the greater or lesser decision-making capacity of the system that integrates them, may have a significant impact on the rights and freedoms of individuals which, as we can see more clearly, go beyond the mere impact on the right to data protection and the right to privacy.

In order to carry out a first approach to the fundamental rights affected, we could start with an analysis of different texts, such as our Constitution, the European Convention on Human Rights[52], the Universal Declaration of Human Rights[53] or the International Covenant on Civil and Political Rights[54]. Also for the purposes of providing an overview, we can highlight the observations of the White Paper on AI in Europe[55], which literally states: *"... The use of artificial intelligence may affect the values on which the EU is founded and*

[50] N.B.: RGPD en relación a los artículos 13.2 f) , 14.2 g) y 15.1 h).

[51] COMISIÓN EUROPEA, "Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica", Informe a la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones, COM(2020) 64 final, 19 de febrero 2020, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0064

[52] CONSEJO DE EUROPA, Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, Roma, 4 de noviembre de 1950.

[53] NACIONES UNIDAS, Declaración Universal de los Derechos Humanos, 217 (III) A. Paris, 1948.

[54] NACIONES UNIDAS, Pacto Internacional de Derechos Civiles y Políticos. Resolución 2200 A (XXI) de la Asamblea General, 16 de diciembre de 1966.

[55] COMISIÓN EUROPEA, Libro Blanco sobre la inteligencia artificial..., op. cit., pág. 13.

lead to the infringement of fundamental rights, such as freedom of expression, freedom of assembly, human dignity, freedom from discrimination on grounds of sex, race or ethnic origin, religion or belief, disability, age or sexual orientation, and, in its application in certain areas, the protection of personal data and privacy, the right to an effective remedy and to a fair trial, or the protection of consumers.".

IMPROVING DESIGNS

If we are able to translate a situation or problem into a mathematical model with variables that can be monitored and can produce output data, by using Artificial Intelligence algorithms we can control and improve that situation or problem. That is, we can teach the model based on past results (from the data we already have), with the aim of making predictions by presenting new input data.

There are many applications that represent examples of healthy Artificial Intelligence that has no detrimental effects on people. One of them is the Moneyball methodology[56] developed in 2001 by Oakland Athletic baseball coach Billy Beane. Using innovative analytical and predictive techniques, he and his collaborators built a low-budget team that had to compete with much bigger teams. These techniques, which were unique to them at the time, showed that the decisions that had been made in the baseball world up to that point were misleading and even irrational. With this information they changed the strategy and focused the selection of players on those coming from the college leagues instead of signing older players whose salaries were very high. As a result of such decisions, Billy Beane took his team to the finals that year, beating teams with much bigger budgets.

Moneyball represents a healthy use [57] of Artificial Intelligence because it complies with the following principles:

- It is a transparent model that anyone can understand and the training data of the algorithms is available to everyone[58].
- It has statistical rigour: data scientists have at their disposal a huge catalogue of training data, and this data is relevant to the outcomes they are trying to predict.
- The data is being updated daily by fans around the world, so scientists can compare the results with the predictions made by their models and see where they have failed.

Not all AI-based applications follow these principles and many of them do not have the same rigour in selecting training data to be massive and relevant, leading to situations of bias that can have serious consequences for the people affected.

One example is the COMPAS tool, used by the American judiciary to analyse the risk of recidivism of a convicted person. Judges across the country rely on it to make decisions about the future of prisoners. This

[56] N.B.: vid. Moneyball: The Art of Winning an Unfair Game, autor Michael Lewis, 2003.

[57] Cathy O'Neil afirma que "El béisbol es un caso práctico sin efectos perniciosos y nos servirá de ejemplo positivo con el que comparar los modelos tóxicos o ADM que están aflorando en tantísimas áreas de nuestra vida". O'Neil, C., Armas de destrucción matemática, Ed. Capitán Swing, 2017, p.27.

[58] N.B.: Los datos de los partidos de béisbol han sido recogidos desde hace más de 100 años por fans de este deporte, y están disponibles a través de diferentes webs como https://sabr.org/how-to/statistical-databases-and-websites

tool, based on convicts' responses to a 137-question assessment, caused controversy when it was discovered in 2014 that it carried a racist bias. While the predictions were correct to a large extent (it correctly classified a person who might or might not reoffend), when errors occurred they were mainly in black people and to a much lesser extent in white people[59]. When this behaviour was discovered, the company behind the solution refused to disclose the details of the algorithm, claiming competition concerns. Despite the criticism received, the tool continues to be used with restrictions (it is made clear that it is a black box, that there are doubts about the validity of the results, that it should in no case replace the judgement of a human, that it must be constantly monitored...).

Another example of an AI-based application with a negative impact on people is the case of TAY, the chatbot designed to mimic the speech patterns of a 19-year-old American teenager, which was launched on 23 March 2016. Apart from providing initial training, the possibility was left open for the chatbot to continue learning through early interactions with human Twitter users. The result was that, within a few hours, the chatbot was responding to other users' messages with sexually and racially charged comments. After several attempts to contain the situation, it was decided to close the account associated with the chatbot after only 16 hours of operation[60]. Researchers explained that this behaviour was understandable since inappropriate behaviour had not been defined yet.

The above are examples of Artificial Intelligence implementations that if they are not carefully reviewed can lead to negative consequences for individuals. The main reason, if we compare their implementation to that of the Moneyball methodology, is that the training data that have been used are much more limited (in COMPAS they have been based on interviews with few questions, in TAY the data have been messages mainly from Twitter Trolls, ...) and that the model is deficient in terms of transparency, being impossible to know why certain decisions have been taken. Cathy O'Neil's book Weapons of Math Destruction[61] compiles a large number of examples of AI that have long been relevant in people's lives (job performance evaluation, insurance pricing, ...), especially in American society.

PART 3: Legal impacts

1. Fundamental rights in the digital society.

The personal data protection is a fundamental right that is not limited to the most intimate data, but extends to any type of personal data, whether intimate or not. In other words, "*all data that identifies or allows the identification of the person, and may be used to create an ideological, racial, sexual, economic or any other kind of profile, or that may be used for any other purpose which in certain circumstances constitutes a threat to the individual*" (Constitutional Court Judgement 292/2000, 30 November 2000).

[59] THE GUARDIAN, "Rise of the racist robots – how AI is learning all our worst impulses", por Stephen Buranyi, 8 de agosto de 2017, https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses https://www.nytimes.com/2017/10/26/opinion/algorithm-compas-sentencing-bias.html>.

[60] https://www.xataka.com/robotica-e-ia/microsoft-retira-su-bot-de-ia-despues-de-que-este-aprendiera-y-publicara-mensajes-racistas

[61] O'Neil, C., Armas de destrucción matemática, Ed. Capitán Swing, 2017.

When carrying out any operation involving the processing of personal data, the requirements derived from legislation on the protection of personal data must be observed.

The development and integration of IoT, Big Data and Artificial Intelligence technologies are an undeniable reality for companies and require, as a budget**, a free flow of data**, whether personal or not. This is why Regulation 2018/1807 on a framework for the free movement of non-personal data in the European Union[62], was approved and fully applicable from May 2019.

Both rules respond to the need to create a clear policy and legal framework adapted to the data economy, removing the remaining barriers to data flow and addressing the legal uncertainties created by new data-driven technologies, as set out by the European Commission in its *Communication Building a European Data Economy*[63]. In fact, Recital 13 of the Regulation states that *"the proper functioning of the internal market requires that the free flow of personal data within the Union should not be restricted or prohibited on grounds relating to the protection of natural persons with regard to the processing of personal data..."*[64].

The debate on human rights in ICTs is usually monopolised by privacy and data protection; however, it is worth remembering that our Constitution recognises other fundamental rights that are protected at the highest level. Nevertheless, even within the framework of such fundamental rights located in the same systematic space of the Constitution, in situations of conflict between them, there are variable intensities, which are deduced from their intrinsic and extrinsic limits. It is clear when we are faced with a collision between the right to life and the right to privacy, but there are other cases in which there is a collision that must be weighed up, for example when the right to freedom of information and the right to privacy collide. In this sense, STC 24/2019, of February 25, reminds us of its doctrine in cases of collision between the right to freedom of information and the right to privacy, stating that: "In relation to the latter fundamental right to privacy, this Court has understood that the public relevance of the information "justifies the requirement to assume the disturbance or inconvenience caused by the dissemination of a particular piece of news"[65].

Therefore, we reassert that the debate should not be limited to the impact on privacy and data protection, but also to the other fundamental rights involved, as can be seen from the General Data Protection Regulation itself, which reiterates in a finalist manner, the need to protect the fundamental rights and freedoms of individuals beyond the strict protection of their personal data. This person-centred approach is also defined in the context of AI as anthropocentric, as acknowledged by the European Commission[66] and should radiate to the systems that serve its purpose, i.e., IoT devices and Big Data systems.

---

[62] LOZA CORERA, M., "Hacia la economía de los datos europea: nuevo reglamento europeo 2018/1807", *Govertis Advisory Services*, 10 de diciembre de 2018, https://www.govertis.com/hacia-la-economia-de-los-datos-europea-nuevo-reglamento-europeo-2018-1807#_ftn3

[63] COMISIÓN EUROPEA, "La construcción de una economía de los datos europea", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM (2017) 9 final, 10 de enero de 2017.

[64] Op. Cit., AEPD, *Código de buenas prácticas*....

[65] TRIBUNAL CONSTITUCIONAL, Sentencia 24/2019, de 25 de febrero, FJ 5, http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/25869#complete_resolucion&fundamentos

[66] COMISIÓN EUROPEA, Directrices éticas para una IA fiable, Grupo de expertos de alto nivel en Inteligencia Artificial, abril de 2019. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

This is why we must not only consider privacy risks, but also risks to our own personal security and potential personal damage, as well as physical damage to our property. For example, according to recent vulnerability analyses of smart home products, attackers could unlock IoT doors and locks, manipulate smart thermostat temperatures beyond factory maximums, etc., so we need to work from the design of these solutions to prevent any of this from happening[67].

In the context of the development of the three technologies mentioned above, to the extent that they integrate a system intended to intelligently manage a task or objective, in many cases risk considerations, given the dependencies generated between them, make it necessary to carry out a global consideration of the risks[68]. For instance, as we warned when we talked about biases, the defects in the decision-making biases of an artificial intelligence system may not be caused directly by the algorithms or logic applied, but by the data itself collected through IoT devices, perhaps in a defective way or with a certain bias, and these biases are precisely amplified when dealing with Big Data techniques, thus causing a bias in the final decision of the AI system. In fact, as the European Commission points out, there are increased risks due to the complexity of products and services when they interrelate with others, for example, in the context of products for our smart home, the design of the AI that manages that home must not only take into account its own performance risks but also take into account the risks of integration of other products, in this particular example, clearly the IoT devices that may eventually be connected to the smart home management system.[69].

Whereas it is true that, as discussed in this report, advances in AI, together with Big Data and IoT, are particularly promising in the field of individual Health and Wellbeing, there are also risk situations that must be taken into account to avoid a detrimental impact on fundamental rights, such as undue discrimination on the basis of an individual's health, which is particularly serious in the context of possible global pandemics such as that caused by COVID19 , or the biased exclusion of individuals, for example, when taking out life or health insurance.

More related to the field of the **right to life** in the very strictest sense, the existence of military applications that, by means of AI systems, select and execute human targets without human intervention, through the so-

---

[67] TSCHIDER, Ch., "Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence", *96 Denv. U. L. Rev. 87 Age*, marzo de 2018, pág. 120.

[68] COMISIÓN EUROPEA, "Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica"..., *op. cit.*

N.B.: *"...Otros riesgos adicionales que pueden afectar a la seguridad son los derivados de la complejidad de los productos y los sistemas, ya que una serie de componentes, dispositivos y productos pueden integrarse e influir en el funcionamiento de los otros (p. ej., productos que forman parte de un ecosistema doméstico inteligente). Esta complejidad ya se trata en el marco jurídico de la Unión en materia de seguridad (...).* ***En concreto, cuando el productor lleve a cabo la evaluación del riesgo del producto, debe considerar el uso previsto, el uso previsible y, en su caso, el mal uso razonablemente previsible. Por ello, si el productor prevé que su dispositivo estará interconectado e interactuará con otros dispositivos, debe considerar estos aspectos en la evaluación del riesgo****. Los usos o malos usos se determinan sobre la base, por ejemplo, de la experiencia de usos pasados del mismo tipo de producto, las investigaciones de accidentes o el comportamiento humano. La complejidad de los sistemas también se trata más específicamente en la normativa sectorial de seguridad, como el Reglamento sobre los productos sanitarios y, en cierto grado, la Directiva relativa a la seguridad general de los productos.* ***Por ejemplo, el productor de un dispositivo conectado, destinado a formar parte de un ecosistema doméstico inteligente, debe poder prever razonablemente que sus productos tendrán un efecto en la seguridad de otros productos*** *(...)".*

[69] Ibidem.

called LAWS (Lethal Autonomous Weapons), have brought to light ethical conflicts on the part of the Commission[70] and the European Parliament[71].

The European Commission has also expressed its views on safety in the production of AI, IoT and robotics systems, indicating that, although much of the legislation, both general and sectoral, was passed before such technologies were emerging[72], the regulatory framework for product safety is technology neutral, so that the application of the product safety framework cannot be excluded, yet it is essential that these technologies are incorporated into the legislative frameworks for civil liability.

Regarding the fundamental right to **equality and non-discrimination**, it should be kept in mind that the right to equality is a generic right, which is asserted in the context of other rights. On the other hand, it is important to remember that the form in which discrimination occurs can be direct or indirect. Direct discrimination is due to unfavourable treatment of a person on the basis of race, sex, sexual orientation, gender identity or other personal or social grounds. Indirect discrimination is based on apparently neutral provisions, criteria or practices that may result in unfavourable treatment of a person on grounds of race, sex, sexual orientation, gender identity or other personal or social grounds.

Although it is true that an instruction or evaluation system of an algorithm that includes direct racial discrimination may be obvious, various authorities and reports have shown that the real risk in this regard is precisely that through biases, indirect discrimination is generated. Either because the data are collected from sources that have already been elaborated or constructed on the basis of an existing bias, or because discrimination is established on a parameter that is apparently not racist or sexist, but which affects an extremely high percentage of a given ethnic, racial or gender group, causing for practical purposes discrimination to the detriment of that group[73].

In relation to the right to freedom of expression, the different preventive systems that content sharing platforms use, for example, to prevent infringement of the terms and conditions of their services, are currently well known. While there is some social acceptance of these systems in that they can prevent certain actions that are commonly considered internationally reprehensible, such as child pornography or the glorification of terrorist acts, it is no less true that there are preventive filtering systems that have aroused more controversy, such as those related to content creation platforms and the existence of algorithms and systems for detecting user works that may infringe the intellectual property rights of third parties. The question of this growing capacity of AI systems that are capable of preemptively filtering content that may be "uploaded" to the network undoubtedly raises legal questions about the scope of the concept of "prior censorship", prohibited by our Constitution [74].

---

[70] COMISIÓN EUROPEA, Ethics Guidelines for Trustworthy AI (draft), op. cit.

[71] PARLAMENTO EUROPEO, Resolución del Parlamento Europeo, de 12 de septiembre de 2018, sobre los sistemas armamentísticos autónomos, https://www.europarl.europa.eu/doceo/document/TA-8-2018-0341_ES.html

[73] EL PAÍS, "Amazon prescinde de una inteligencia artificial de reclutamiento por discriminar a las mujeres", por Isabel Rubio, 12 de octubre de 2018, https://elpais.com/tecnologia/2018/10/11/actualidad/1539278884_487716.html

[74] ESPAÑA, Constitución Española, BOE 29 de diciembre de 1978, artículo 55.

As for the right to freedom of information, as passive subjects, we have already been warned at the institutional level about the risk of entering echo chambers or, as we mentioned in relation to biases, bubble filters[75]. The increasingly detailed personalisation of the user profile used by search engine services can lead to the user only receiving the information that the AI system understands that he/she will like, in accordance with the patterns expressed by the user or even in accordance with the interests of third parties that may influence the management of the different algorithms used by the search engines.

In relation to the right to free elections, and democratic political systems, can elections in which voters' perceptions are manipulated in order to make them vote one way or the other be considered free? Perhaps we should first define at what point could we speak of vote canvassing, election campaigning or outright manipulation?

In this regard, the aforementioned cognitive biases, which can be enhanced, for example in the field of politics, through Big Data systems that profile large volumes of voters and ideological segments[76] through their interactions in social networks and through other AI tools, are of particular importance for the purposes of possible manipulation, such as the automated generation of fake news, Deep Fakes, Bots or other mechanisms, with an increasingly greater capacity for deception, to direct messages and political marketing campaigns that are increasingly personalised and perfected, leaving the suitability of the candidate or political proposal in the background and opting for particularly aggressive marketing systems[77]. s we can see, the impact is not only in the context of freedom of information, but also has a direct impact on the democratic system itself[78] with special vulnerability for those systems of direct election (consultative processes or referendums, systems of direct election of the candidate, etc.).

2. Specifying privacy risks

In terms of personal data protection, the regulatory requirements derive from **General Data Protection Regulation 679/2016**, hereinafter GDPR, complemented in the national case by Organic Law 3/2018, of 5 December, on Personal Data Protection and guarantee of digital rights (LOPDGDD in spanish), which is based on the premise[79] that data protection cannot be an obstacle to the proper functioning of the internal market, and all this without compromising on the standards of protection to guarantee this right:

[75] CONSEJO DE EUROPA, "Algorithms and human rights - Study on the human rights dimensions of automated data processing techniques and possible regulatory implications", Committee of experts on internet intermediaries (MSI-NET), 2018, https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html

[76] TRIBUNAL CONSTITUCIONAL, Declaración inconstitucionalidad artículo 58bis LOPDGDD, vid. SENTENCIA 76/2019, de 22 de mayo, https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_076/2019-1405STC.pdf

[77] **N.B.:** *Puede citarse también el conocido caso de Cambridge Analytica, vid.* https://www.xataka.com/privacidad/el-escandalo-de-cambridge-analytica-resume-todo-lo-que-esta-terriblemente-mal-con-facebook

[78] THE GUARDIAN, "The great British Brexit robbery: how our democracy was hijacked", por Carole Cadwalladr, 7 de mayo de 2017, https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy

79 N.B.: En el considerando 13 RGPD se dice así: "El buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales".

> *Technology has transformed both economic and social life and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of protection of personal data.* [80]

Concerning the GDPR, we highlight **consent, transparency and purpose limitation** in the processing of personal data.

Both the GDPR and the well-known **ePrivacy**[81], **Regulation proposal** establish the maximum guarantees for obtaining the user's free consent[82] and transparency[83] regarding the processing of our information in electronic communications. Nor should it be overlooked that the purpose of the processing must be limited to the purpose for which it is intended and the user must be duly informed, among other things, whether or not such processing requires his or her consent.

BIG DATA

The impact on privacy rights in the field of Big Data is clear. Firstly, the duty of information must be complied with and, in the case of requiring consent as a basis for legitimisation, it must be properly obtained and managed for the data subject, so transparency plays an essential role, which is not always easy to articulate in an operational manner if we take into account the high volume of data subjects that can potentially feed the Big Data system. The AEPD points out that a possible legal risk may be the subsequent use of data acquired for a specific purpose, which are then reused for another purpose of which the data subject was not informed.

Likewise, the generation of profiles or profiling can be identified as one of the main risks associated with this technology, as pointed out by the Spanish Data Protection Agency (AEPD)[84]. A risk that, we understand, is not only related to the simple generation of profiles, but also to the fact that the typology of profiles can be used in predictive models, or even in AI systems. Subsequently, they would generate discrimination or introduce harmful biases for certain population groups, with the aggravating circumstance that they are particularly vulnerable groups.

Another element to be considered is the different origin of the data from different sources, with a greater complexity of actors involved in the process, and therefore the existence of controllers, co-responsible parties and/or processors, whose relationships must be suitably regulated and to ensure, especially the data

---

[80] MERCADER UGUINA, J. R., "El futuro del trabajo y el empleo en la era de la digitalización y la robótica", En: DE LA QUADRA-SALCEDO, T., PIÑAR MAÑANAS, J. L. (Dirs.), Sociedad digital y Derecho, Madrid: BOE, 2018, pág. 617,

https://www.boe.es/publicaciones/biblioteca_juridica/abrir_pdf.php?id=PUB-NT-2018-97

[81] COMISIÓN EUROPEA, Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), 2017/0003(COD), 10 de enero de 2017, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010

[82] N.B.: vid artículos 7 y 8 RGPD, y 9 Reglamento ePrivacy.

[83] N.B.: vid artículos 13, 14 RGPD y artículo 10 Reglamento ePrivacy.

[84] AEPD, Código de buenas prácticas..., op. cit.

controller, that it diligently chooses the corresponding supplier or partner for the processing of such data and that the latter act with the due diligence. Provisions on the retention and re-use of data will also be key.

INTERNET OF THINGS

The challenges in terms of personal data protection within the Internet of Things sector have already been highlighted by the Article 29[85] Working Party and consist of articulating the correct mechanisms for users of this type of services to keep their personal data under their complete control, throughout the entire life cycle of the product or service, always with their free, informed and specific consent. This is why the right to data protection is the first to be impacted by this technology.

IoT technology is based on providing services that have a high impact on people's lives by capturing a large amount of data that can be highly sensitive. The multi-lateral interaction of connections generates a complex data flow that is difficult to handle with user tools.[86]

In addition, the complexity of this type of services may imply that the communication between the different objects involved in the Internet of Things is activated automatically and by default, without the user being aware of this fact. In essence, it is necessary to protect the user so that in the interaction of the objects he/she can define how he/she wants to control the generated data flow. In this sense, if the user is not able to control this flow in its first stage, it will be difficult for the user to control the later stages where the data is processed outside its area of influence and where, at the same time, can interact with other technological advances such as Cloud Computing or Big Data[87].

ARTIFICIAL INTELLIGENCE

In the area of AI, given the need to process large amounts of data, it applies the privacy risks mentioned in the previous sections on Big Data and IoT.

As the Spanish Data Protection Agency (AEPD)[88], "states, "the person who makes the decision to carry out the processing is responsible and cannot hide behind a lack of information or lack of technical knowledge to evade their responsibility when it comes to auditing and deciding on the suitability of the system". This is why it is essential that, before implementing an AI-based solution, the necessary privacy measures are adopted from the design stage and, by default, the corresponding Data Protection Impact Assessments or, where appropriate, Risk Analyses are carried out. As the AEPD also states[89] "what is not acceptable under any circumstances is to shift the responsibility to the IA system itself".

---

[85] GT29, Dictamen 8/2014..., op. cit.

[86] SANTAMARÍA RAMOS, F. J.: "Internet de las cosas: un desafío para la protección de datos personales", Actualidad Administrativa nº 7-8, julio-agosto 2015, págs. 40-57.

[87] Ibidem.

[88] AEPD, Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial..., op. cit., pág. 19.

[89] Ibídem.

It will therefore be essential to comply with the duty of transparency and information towards the data subject and to inform him or her, in the case of automated decisions, including profiling as referred to in Article 22(1) and (4) of the GDPR, and at least in such cases, that it is meaningful information on the logic applied, as well as the significance and the intended consequences of such processing for the stakeholders.

PART 4: Technology impacts.

1. General security risks.

Since 2006, the World Economic Forum has annually presented the document "Global Risk Report", in which it lists the main risks to be faced worldwide, classified according to their probability and impact. Technological risks regarding information security already appeared in the first editions of the report, but it was in the 2012 report that the risk of cyber-attacks was defined, ranking it at that time at the top in terms of probability of materialising.

In the 2020 report, the World Economic Forum reiterates the need to create a strong culture of cyber security and in the 2021[90] report, cyber security flaws swell the list of risks most likely to have a negative impact in the next ten years. The volume of data processed will be ever-increasing and will grow at great speed with the spread of disruptive technologies such as blockchain, quantum computing, ubiquitous connectivity (which will emerge with the deployment of 5G) or the needs arising with the consolidation of the new industrial revolution. Just as these new technologies will support socio-economic progress, the risk of cyber-attacks for each of these new scenarios will increase in frequency and impact.

In this context, cyber security must, besides preventing internal and external threats, be able to detect attacks in real time in order to respond quickly and appropriately to minimise damage.

The adoption of technologically innovative solutions based on what are known as disruptive technologies brings with it new security risks arising from the lack of maturity of protection measures.

With the massive deployment of IoT devices, both at business and home level, the area of exposure increases considerably. This means that the perimeter to be protected is becoming larger and larger, to the point of becoming the device itself: more assets, more and larger wireless networks, and with different protocols (Bluetooth[91], LoRa[92], NB-IoT[93], SigFox[94], etc.), which makes the need to adopt security by design and security by default particularly important. Likewise, this disappearance of the concept of the perimeter as a trusted

[90] World Economic Forum, The Global Risks Report 2021, 16th Edition, http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

[91] N.B.: Tecnología de acceso inalámbrico para la transmisión de datos por radiofrecuencia entre aparatos.

[92] N.B.: Tecnología inalámbrica que emplea un tipo de radiofrecuencia patentado por Semtech; como tipo de comunicación, encuentra usos militares y espaciales.

[93] N.B.: Narrowband-IoT es una tecnología útil para objetos cotidianos que requieren pequeñas cantidades de datos en períodos de tiempo largos.

[94] N.B.: Se trata de otra tecnología de conectividad en Internet de los objetos.

zone has meant that prevention measures, which were predominant in cyber security strategies a few years ago, have gradually given way to measures based on detection, response and recovery in the event of incidents.

As with Big Data, Artificial Intelligence introduces security and privacy risks associated with massive data processing and analysis tools. AI also plays an active role in security, as it can be used in applications to detect and respond to cyber-attacks or, in the opposite case, as an ally of cyber-attackers. It is not news[95] that cybercrime is embracing advances in AI and automation to market new threats to attack critical infrastructure. In this sense, there is a technological race on both sides to develop the best solutions and products. Cybercriminals have numerous resources at their fingertips, which means that the variety and complexity of threats that benefit from this technology is increasing enormously.

Some threats arising from the use of Artificial Intelligence by cyber criminals include [96]:

- The use of Machine Learning techniques to design search models and prioritisation of targets to attack, analysing access characteristics and current protection measures.
- Neuroscience techniques, because they allow the development of tailor-made malware, optimising social engineering deception techniques to convince users to access a certain resource where personalised malware awaits them.
- The use of Advanced Intelligent Threat techniques for the development of intelligent malware.
- The use of Artificial Intelligence applications to manipulate videos and/or images of celebrities and then disseminate them through social networks, creating *fake news*[97] or *deep fakes*[98].

Seven out of ten companies[99] re already using some form of Artificial Intelligence for asset protection. The main application is in detection tasks (of fraud, security leaks, advanced malware, etc.), reducing the time to detect a security breach and saving on the detection and response costs themselves.

For its part, Cloud technology[100], as an essential element of Big Data and AI-based solutions, as a storage solution, introduces the risks inherent in the outsourcing of services (security and privacy risks) and those derived from data access control.

---

[95] JUANES, C., DE FUENTES, J.M., SAN JOSÉ, J., "Ciberseguridad: Inteligencia artificial para garantizar la mejor defensa", Marketing y Ventas, núm. 161, mayo de 2020.

[96] Ibidem.

[97] N.B.: En castellano, bulo.

[98] N.B.: Técnica de inteligencia artificial que permite editar vídeos haciendo creer que las personas que aparentemente son reales, utilizando para ello algoritmos de aprendizaje no supervisados a partir de vídeos o imágenes ya existentes.

[99] CAPGEMINI RESEARCH INSTITUTE, "Reinventing Cybersecurity With Artificial Intelligence", 2019, https://www.capgemini.com/es-es/wp-content/uploads/sites/16/2019/07/AI-in-Cybersecurity_Report_20190710_V05.pdf

[100] N.B.: Computación en nube; tal y como la define la RAE, modelo de prestación de servicios tecnológicos que permite el acceso bajo demanda y a través de internet a un conjunto de recursos compartidos y configurables de modo escalable (como redes, servidores, capacidad de almacenamiento, aplicaciones y servicios, etc.).

Until the emergence of the disruptive technologies, the protection of an organisation's information assets was limited to the IT area. A company's data used to be processed and stored in the company's servers (physical or virtual), servers normally located in the company's Data Centre, or in an external Data Centre, in the form of hosting, at the most. This IT area controlled the corporate equipment (desktops or laptops) from which the information was accessed and the data transferred could be monitored, either through e-mail (the mail server could be in the company itself) or through other communications networks (a firewall could control the only access point from outside the company, through VPN, for example).

This scenario has changed completely in recent years. Cloud Computing has made it possible to get rid of physical corporate servers, shifting acquisition and maintenance costs to a service cost, and introducing the concept of on-demand service or provisioning. Savings in storage costs have enabled the widespread use of Big Data, which has led to the deployment of advanced analytics capabilities in the Cloud at reasonable costs. Mobility, interconnection, 4G networks or the future deployment of 5G or connected objects have completely blurred the corporate perimeter, multiplying the number of access points to information. As noted in the previous section, all of this brings with it common security risks: greater exposure, dependence on security guarantees from external service providers and diversity of the systems to be protected.

Protection systems are also evolving to meet new technological needs. We have gone from traditional firewalls based on source/target rules to Next Generation Firewalls (NGFW); from signature-based antivirus to EDR (Endpoint Detection & Response); or we have incorporated complete solutions for the protection of SaaS services[101] in the Cloud, known as CASB (Cloud Access Security Broker).

Even other disruptive technologies, such as Blockchain, can help to increase security in the face of the challenges faced by these same technologies (such as those we are dealing with: Artificial Intelligence, Internet of Things, Big Data). Indeed, Artificial Intelligence is characterised by helping or even automating decision making based on the claim of optimising the mental processes that would determine the most correct decision[102], and on the other hand Blockchain helps us to verify, execute and record the different digital transactions that are carried out. Both technologies complement each other perfectly and their use can undoubtedly bring great benefits to the security of systems: Artificial Intelligence provides analytics and information to decision-making processes, and Blockchain provides integrity, security and decentralises the environment in which transactions take place, which can contribute enormously to the improvement of processes.

[101] N.B.: Software como un Servicio (Software as a Service) es un modelo de distribución de software donde el soporte lógico y los datos que maneja se alojan en servidores de una compañía de tecnologías de información y comunicación, a los que se accede vía Internet desde un cliente.

[102] PWC IDEAS, "Inteligencia artificial y Blockchain, el yin y el yang de la tecnología", 2016, https://ideas.pwc.es/archivos/20161111/inteligencia-artificial-y-blockchain-el-yin-y-el-yang-de-la-tecnologia

2. Specific security risks.

INTERNET OF THE THINGS

The National Institute of Standards and Technologies (NIST) published NISTIR 8228[103] on the identification and management of privacy and cyber security risks in IoT devices in 2019. It classifies risks according to those related to device security, data security and individual privacy. Among the main security risks identified in IoT, the following can be mentioned:

- Lack of management and administration capacities
- Lack of monitoring and tracking capabilities (logs)
- Lack of user interfaces (or not fully functional)
- Difficulty of centralised management
- Wide variety of software to manage
- Short life cycle of devices
- Lack of technical documentation on the devices (difficult to repair)
- Lack of IoT inventory tools
- Numerous stakeholders for the same service (device manufacturer, App manufacturer, cloud service provider, telecommunications provider, etc.)

On its part, the Spanish Data Protection Agency [104] has listed the main risks to privacy and data protection in the IoT field:

- Invasive disclosure of behavioural patterns and profiling
- Lack of control and asymmetry of information
- Involvement of multiple stakeholders with different roles of responsibility, leading to difficult levels of compliance, which in turn can lead to further security vulnerabilities that can result in a security breach of personal data.
- IoT systems can affect not only the direct users of the systems but also those who may at some point be 'in proximity' to the system or device.
- Lack of appropriate security measures at any of the layers (device, communication and service), either due to the limitations of the devices, or due to deficiencies in the application of data protection principles from the design, such as lack of encryption in communications, default passwords, etc. The Spanish Data Protection Agency (AEPD) points out that this lack of security measures can lead to the exploitation of vulnerabilities in the device, allowing, for example, its remote manipulation or offensive uses (DDoS) or direct attacks on the application layer involving improper access to users' personal data or actions that lead to a breach of security.

[103] NIST, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks", NISTIR 8228, junio de 2019, https://csrc.nist.gov/publications/detail/nistir/8228/final

[104] AEPD, IoT (I): Qué es IoT y cuáles son sus riesgos, 3 de Diciembre de 2020, https://www.aepd.es/es/prensa-y-comunicacion/blog/iot-i-que-es-iot-y-cuales-son-sus-riesgos

- Limitations or inability to remain anonymous, due to issues such as the use of unique identifiers and the linkage of these between devices.

The Spanish Data Protection Agency (AEPD) has also warned of the risks of IoT in the field of health, which has given rise to the Internet of Bodies[105]) defined as the "use of devices connected to the Internet that monitor and/or act on all or some of our vital signs and other biometric data, as well as other health indicators such as physical activity, sleep quality, sporting activity or sedentary lifestyle". An attack on this type of device can have serious consequences for people's health, so, as the Spanish Data Protection Agency indicates, the reliability, robustness and resilience of all the processing in which the devices are framed must be as high as possible.

ARTIFICIAL INTELLIGENCE

As can be seen from previous sections of this study, the risks of the use of Artificial Intelligence are not only related to device or communication risks. From the European Commission's point of view, the main risks arising from the use of Artificial Intelligence are related to its consequences in terms of personal data protection, privacy, personal security or civil liability[106].

In this sense, we can say that Artificial Intelligence is distinguished from other technological disciplines by its capacity for self-learning through training data and by the criticality of the decisions it can take. Training data may present biases, especially in terms of security, with unauthorised access to such data with the aim of influencing the predictions or decisions that can be inferred.

More specifically, the Spanish Data Protection Agency (AEPD) has pointed out some security threats in processing operations that incorporate Artificial Intelligence:

- Attacks using adversarial pattern poisoning techniques through access and manipulation of training data sets, prior to model configuration.
- Trojans and backdoors in the code itself or in the development tools.
- Access to the model, both at black box and white box level for manipulation of model parameters, filtering the model to third parties or attacks on the integrity or availability of inferences.
- "Adversarial machine learning" referred to by the Spanish Data Protection Agency (AEPD) as techniques for feeding example data that to our perception as humans may be indistinguishable from normal data, but which include small perturbations that force the AI to make incorrect inferences.
- Attacks by imitation of patterns that are already known to be supported by the AI.
- Possibility of re-identification of personal data included in the model by membership inference or inversion of the model itself.
- Fraud or deception of the AI system by data subjects to the detriment of others.

[105] AEPD, IoT (II): Del Internet de las Cosas al Internet de los Cuerpos, 11 de Enero de 2021 https://www.aepd.es/es/prensa-y-comunicacion/blog/iot-ii-del-iot-al-iob

[106] COMISIÓN EUROPEA, Libro Blanco sobre la inteligencia artificial, op. cit.

- Loss of confidentiality of profiling results or decisions inferred by the AI as well as logs resulting from inferences generated in the interaction with stakeholders[107].

On the other hand, ENISA also has a specific document on AI-related risks, which provides a taxonomy of high-level threats that includes 8 categories, including, among others, Fraudulent Activity, Espionage/Interception or also Physical Attacks, Disasters or Disruptions. Within these high-level categories, up to a total of 74 threats are included, e.g., for Fraudulent Activity, threats relating to Model Sabotage or AI Model Poisoning are identified, or, among others, for Interception/Espionage, AI Model Disclosures, Data Inference or Weak Encryption[108], among others.

Some practical examples of some of the security risks mentioned above include evading anti-spam systems by changing characters: for example, entering the number "1" instead of the letter "i" to obtain "V1agra" (although this is now detected as spam) A much more serious potential problem would be solutions with impacts on user health, due to one of the characteristics noted above: Artificial Intelligence algorithms are used for extremely critical decision-making. For example, in autonomous cars relying on artificial vision techniques, the images received by such systems could be manipulated (by removing a STOP sign on a road) and thus cause an accident. Similar examples of fraud could occur in recruitment processes, by including false merit keywords in a CV, in a font and colour invisible to the human viewer, but readable by the AI system and effectively processed through its pre-filters, thus ruling out other candidates or putting the candidate at an unfair advantage over other candidates[109].

Finally, it should be noted that, as stated in the aforementioned White Paper of the European Commission, most Artificial Intelligence technologies are based on a "black box effect"[110] and partially autonomous behaviour, aspects that do not help to verify how a given decision has been carried out.

These characteristics of Artificial Intelligence make it extremely difficult to carry out an effective review to verify whether or not the decision-making process complies with Data Protection regulations. Hence the importance of advancing in techniques to discover the root cause of the errors that Artificial Intelligence may cause both in terms of the levels of availability and quality of the data, as well as the learning algorithms used. Review facilities are also important to prove cause-effect relationships between technological action and an outcome, especially when it causes harm to third parties. The latter fits into the general need for monitoring and management of events (logs) on devices, especially in converged IoT-IA systems.

Algorithmic audits are particularly important here in order to prevent security, ethical and legal risks.

---

[107] AEPD, Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción, 2020, p. 42 a 43. https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

[108] ENISA, Artificial Intelligence Cybersecurity Challenges, Diciembre de 2020. https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

[109] AEPD, Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción, 2020, p. 43. https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

[110] N.B.: Es un elemento que se estudia desde el punto de vista de las entradas que recibe y las salidas (interfaz) o respuestas que produce, sin tener en cuenta su funcionamiento interno.

BIG DATA

ENISA has a document that analyses **threats** in Big Data, the, se trata de "*Big Data Threat Landscape and Good Practice Guide*"[111], identifying the following threats:

- Unintentional damage / Loss of information:
  - Data leakages due to human error
  - Data leakages through web applications (insecure APIs)
  - Design or implementation failures
- Espionage / Data interception:
  - Data interception
- Fraudulent activity:
  - Identity theft or impersonation
  - Denial of service
  - Malicious software (malware)
  - Certificate spoofing
  - Unauthorised activities, abuse of privileges
  - Business process failure
- Legal:
  - Non-compliance of regulation or legislation
  - Unauthorised management of personal data
- Organisational:
  - Lack of qualified staff.

In relation to the **risks** in the use of Big Data technology, in addition to the same risks that exist in traditional data processing systems (see ENISA's[112] Big Data Threats document), there are also those resulting from its own characteristics:

- Data scale can provide information accuracy far superior to traditional systems and is therefore a very attractive target for attackers for different purposes (black market sales, extortion).
- This accuracy takes the detail of user profiles built by application owners one step further, thus creating an information asymmetry between the user and the data owners.
- Data collected in Big Data applications, used to analyse critical situations, can be misinterpreted or used inappropriately, e.g. because of an attack with the aim of generating misleading analysis that could be fatal for the companies that use such systems.

[111] ENISA – Big Data Threat Landscape and Good Practice Guide (2016): https://www.enisa.europa.eu/publications/bigdata-threat-landscape/at_download/fullReport

[112] ENISA, Big Data Security Good Practices and Recommendations on the Security of Big Data Systems, diciembre de 2015, https://www.enisa.europa.eu/publications/big-data-security

PART 5: Risk management

We have so far seen the different ethical, legal and security impacts that must be taken into account in the use of disruptive technologies. In this section, we will address risk management, bearing in mind the different impact vectors discussed above.

1. Regulatory compliance.

If there is one thing the Internet of Things, Big Data and Artificial Intelligence have in common, it is that they are technologies that enable us to collect, process and analyse vast amounts of information. As the European Commission[113] has already stated, as data-driven transformation permeates the economy and society, the volumes of data generated by machines or processes based on emerging technologies such as the internet of things, the factories of the future and autonomous connected systems are increasing.

The European Union is aware that data is an **essential resource** for economic growth, job creation and social progress, to the extent that it constitutes the so-called "Data Economy". In the words of the European Commission[114], "the "data economy" is characterised by an ecosystem in which different types of market stakeholders - like manufacturers, researchers and infrastructure providers - work together to ensure that data is accessible and usable. This allows them to extract value from that data, creating a range of applications with great potential to improve everyday life".

For this reason, Europe has been aware of the need for a clear **legal framework** that would allow the free flow of data and access to large datasets within the EU, thus removing potential obstacles to innovation and business creation, and therefore to the Data Economy.

PERSONAL DATA

As mentioned in the section on legal impacts, and specifically in terms of data protection and privacy, we must bear in mind the **General Data Protection Regulation 679/2016 (GDPR)**, complemented in the national case by the Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights (LOPDGDD in Spanish) and the still proposed ePrivacy Regulation as axes that set the basis for the regulatory requirements in this area.

Aspects such as the duty to inform, to obtain consent, transparency and purpose limitation in the processing of personal data are crucial.

From a practical point of view, it is particularly important to analyse how to comply with the **duty to provide information** on data processing in accordance with the **principle of transparency** or, as the case may be, **consent**, as this is a challenge given the physical characteristics of the device. Consider, for example, a connected wristwatch with a small display or a device without a visual interface.

[113] COMISIÓN EUROPEA, "La construcción de una economía de los datos europea", op. cit.

[114] Ibidem

Finally, concerning purpose limitation, it is essential, especially in increasingly complex chains of stakeholders and technological solutions that can integrate an IoT, Big Data and AI system, that there are enough mechanisms and guarantees to ensure that the huge amounts of data provided by users are not used for different purposes that are incompatible with those initially informed to the end user.

NON-PERSONAL DATA

The issue of the free flow of data as a presupposition for the development of the Data Economy concerns all types of data, not only personal data, and the legal framework has therefore been completed with Regulation 2018/1807 on a framework for the free flow of non-personal data in the European Union (Reglamento 2018/1807 relativo a un marco para la libre circulación de datos no personales en la Unión Europea).

It applies[115] to electronic data processing which is not personal in nature, which is provided as a service to users residing or having an establishment in the EU, or is carried out by a natural or legal person residing or having an establishment in the Union for its own needs. This Regulation shall not apply to data processing services taking place outside the EU.

As it can be seen, when speaking of "**electronic data which are not of a personal nature**", a negative definition is provided, so that Regulation 679/2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter, GDPR) will apply when we may be dealing with personal data, according to the definition given by the GDPR. This does not mean that, where personal data are involved, Regulation 2018/1807 ceases to apply, since, as the legal text itself clarifies, where there is a set of personal and non-personal data (by which we mean a differentiated set), Regulation 2018/1807 will apply to the non-personal data and where the data in that set are "inextricably linked", both Regulations will apply.[116].

INTELLECTUAL PROPERTY

The necessary principles of transparency in decision-making by AI systems, already partly anticipated by the GDPR in Article 13, as a necessary information requirement for the data subject: "(...) f) *the existence of automated decisions, including profiling, as referred to in Article 22(1) and (4), and, at least in such cases, meaningful information about the logic applied and the significance and expected consequences of such processing for the stakeholder.* (...)", pose a challenge on the protection of the work and authorship of AI systems, which are sometimes the pillars of different business models and which, without adequate legal protection against spying practices fraudulently disguised as exercises of rights, may lead to significant competitive imbalances in Industry 4.0.

While computer programs may be subject to intellectual property protection, their creation must be original[117], raising additional challenges in the case of an algorithm that is capable of "self-improvement" through

[115] N.B.: Vid. artículo 2.1 del Reglamento 2018/1807.

[116] LOZA CORERA, M., "Hacia la economía de los datos europea...", op. cit.

[117] N.B.: La Ley de Propiedad Intelectual (LPI), en su artículo 96.2 establece: "El programa de ordenador será protegido únicamente si fuese original, en el sentido de ser una creación intelectual propia de su autor".

feedback from other computer codes that may be created by third parties. In the same sense of this capacity for "autonomous" creation that the AI system may develop, other challenges arise, such as the authorship of an artistic work created by an algorithm, since the AI system does not have the legal capacity to be the holder of rights and obligations[118,119].

BUSINESS SECRETS

The enormous information processing capacity of big data systems can generate added content with high added value, e.g. in the form of know-how and information of strategic, economic and competitive value for the operator of the system. In the event that data protection law does not apply, the protection of business secrets legislation may apply[120]. The information that we may collect as a result of Big Data or AI analysis may additionally infer specific, high-value information, for example: market estimates, risks, etc. that may be susceptible to protection under business secrecy regulations, in the sense that it is not normally known or accessible information, as it requires large processing capacities, and therefore has a special business value, for example: if it gives us indicators on how and when to carry out certain economic investments and, finally, conditioned by the above circumstances, reasonable measures are established to maintain its secrecy. Therefore, as we have said, the proper implementation of an Information Security Management System would be critical, not only for the protection of personal data, but also for the protection of information that is not necessarily of a personal nature, but has a high value for the organisation.

CIVIL LIABILITY

One of the issues highlighted by the European Commission, both in its White Paper on Artificial Intelligence[121] and more specifically in its document Liability for Artificial Intelligence and other emerging digital technologies[122], are the new challenges in terms of civil liability arising from the use of AI[123].

---

[118] GUADAMUZ, A., "La inteligencia artificial y el derecho de autor", OMPI revista, octubre de 2017, https://www.wipo.int/wipo_magazine/es/2017/05/article_0003.html

[119] N.B.: Según la LPI, artículo 5: "1. Se considera autor a la persona natural que crea alguna obra literaria, artística o científica.2. No obstante, de la protección que esta Ley concede al autor se podrán beneficiar personas jurídicas en los casos expresamente previstos en ella."

[120] N.B.: La Ley 1/2019, de 20 de febrero, de Secretos Empresariales, que traspone la Directiva (UE) 2016/943, de 8 de junio, define los secretos empresariales como:"(...) cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero, que reúna las siguientes condiciones: a) Ser secreto, en el sentido de que, en su conjunto o en la configuración y reunión precisas de sus componentes, no es generalmente conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesible para ellas; b) tener un valor empresarial, ya sea real o potencial, precisamente por ser secreto, y c) haber sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto.(...)".

[121] COMISIÓN EUROPEA, Libro Blanco sobre la inteligencia artificial, op. cit.

[122] COMISIÓN EUROPEA, Liability for Artificial Intelligence and other emerging digital technologies, Expert Group on Liability and New Technologies, 2019, https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608

[123] N.B.: En este sentido se cita la Directiva del Consejo de 25 de julio de 1985 relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de responsabilidad por los daños causados por productos defectuosos, traspuesta en nuestro ordenamiento jurídico a través de la Ley 22/1994, de 6 de julio, que fue derogada por el actualmente vigente Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. Se citan también la Directiva 2014/104/UE del Parlamento Europeo y del Consejo de

A particularly controversial point, which is also very illustrative of the practical application of AI and legislation, are the so-called **autonomous cars**, especially in cases of civil liability arising from accidents. Neither the European legislative framework nor our national legislation (Royal Legislative Decree 8/2004, of 29 October, approving the revised text of the Law on civil liability and insurance in the circulation of motor vehicles), provides an express response, as is logical due to its historical context. Perhaps one of the closest approximations of our national institutions to the practical context of autonomous vehicles has been on the part of the Directorate General of Traffic (DGT), through the instructions INSTRUCTION 15/V-113 on Authorisation of tests or research trials carried out with automated driving vehicles on roads open to traffic in general [124] and INSTRUCTION 16 TV/89 on Assisted parking of motor vehicles[125].

TRANSPARENCY

Within the public sector, the debate on the transparency of AI decisions and the use of such technology may take on greater significance, especially if we take into account transparency legislation at national and regional level.

According to Law 19/2013, of December 9, 2013, on transparency, access to public information and good governance, "*public information is understood to be the contents or documents, whatever their format or support, which are in the possession of any of the subjects included in the scope of application of this title and which have been produced or acquired in the exercise of their functions*". In view of the above article, if a City Council had developed an AI system to fine for non-compliance with certain ordinances, could we as citizens demand to know the basis of the algorithms of the AI system on the basis of the Law on Transparency? Or would we be able to set limits to prevent that too deep a study of the system could make it easier for citizens to take advantage of its defects and violate the ordinances that the AI is supposed to enforce?

AUDIT AND SECURITY

Data governance tools are an enabler for audits and possible impact analysis. These tools manage the level and type of user access to data resources, as well as the use that each group of users makes of them. Some of them can generate reports that reflect the security implemented at the level of each technological element and the security applied to each role and group of users, being the ideal entry point for a general corporate audit without having to go through the entire infrastructure.

Also important in this area are the audits of algorithms through which we can demonstrate compliance with regulatory requirements both in terms of data protection and the proposed Artificial Intelligence Regulation and other regulations, but also technical and ethical aspects, in line with the provisions of the High-Level

---

26 de noviembre de 2014 relativa a determinadas normas por las que se rigen las acciones por daños en virtud del Derecho nacional, por infracciones del Derecho de la competencia de los Estados miembros y de la Unión Europea, traspuesta en nuestro ordenamiento jurídico a través del Real Decreto-ley 9/2017, de 26 de mayo, con afectación en distintos cuerpos legislativos.

[124] DGT, "Instrucción 15/V-113 sobre autorización de pruebas o ensayos de investigación realizados con vehículos de conducción automatizada en vías abiertas al tráfico en general", op. cit.

[125] DGT, "Instrucción 16 TV/89 sobre estacionamiento asistido de vehículos a motor", Dirección General de Tráfico del Ministerio del Interior, 20 de enero de 2016, http://www.dgt.es/Galerias/seguridad-vial/normativa-legislacion/otras-normas/modificaciones/2016/Instruccion_16_TV_89_Estacionamiento_asistido_vehiculos_motor.pdf

Expert Group on Artificial Intelligence[126] and the seven requirements for reliable AI and of course with the proposed Artificial Intelligence Regulation.

2. Standardisation: ISO and Certifications.

The current in crescendo and unstoppable advance of both present and future uses of disruptive technologies is generating important challenges in different fields, such as social, economic and regulatory.

Aspects related to reliability, security and privacy, together with decision making based on complex data analysis processes or the feared repercussions in the world of work, mean that the different regulatory bodies concerned, as well as governments, are working together and are aware of the need for a coordinated and international approach to this issue.

In the words of José Antonio Jiménez - Electronics and ICT Standardisation Technician*: "Standardisation helps the massive implementation of technological advances in society. At the moment, a revolution is taking place in the incorporation of information technology in all productive sectors, both traditional and newly created. Among the multitude of technologies, two are particularly relevant: Artificial Intelligence (AI) and the Internet of Things (IoT). The introduction of these technologies in the real world faces challenges such as interoperability, security, associated risks, ethical and social implications. For all these challenges, standards provide the solutions needed"*[127].

References in this sense are the working lines and competences of the subcommittees SC41 and SC42 belonging to the ISO/IEC JTC 1 committee [128], an established international reference committee whose purpose is to develop, maintain and promote standards in the field of Information Technology (IT) and Information and Communications Technology (ICT) and which is jointly constituted by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC).

- ISO / IEC / JTC 1 / SC 41: Internet of Things and related technologies.
- ISO / IEC / JTC 1 / SC 42: Artificial Intelligence.

Subcommittee SC 41 was created in 2016 from the merger of two JTC 1 working groups, Sensor Networks (WG 7) and IoT (WG 10). Its role is to support standardisation committees on IoT and related technologies, including sensor networks and wearables. It currently has 18 active work programmes[129] ranging from IoT reference architecture proposals to inter-device compatibility requirements to, for example, IoT and Blockchain integration.

---

[126] High-Level Expert Group on AI, Ethics guidelines for trustworthy AI, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[127] UNE, "Impulso español a las normas mundiales sobre IA, Big Data e IoT", por José Antonio Jiménez, La revista de la normalización española, enero de 2020, https://revista.une.org/21/impulso-espanol-a-las-normas-mundiales-sobre-ia-big-data-e-i.html

[128] ISO, "ISO/IEC JTC 1Information Technology", International Organization for Standardization. https://www.iso.org/isoiec-jtc-1.html

[129] IEC, "ISO/IEC JTC 1/SC 41 Work programme", https://www.iec.ch/dyn/www/f?p=103:23:8187723854992::::FSP_ORG_ID,FSP_LANG_ID:20486,25

The SC 42 subcommittee was created in 2017 with the aim of developing international standards to serve as a reference in the field of Artificial Intelligence ecosystem development. The topics that are included in the scope of this subcommittee's work are: Fundamental standards, computational approaches and IS features; use cases and applications; Big Data and Societal concerns[130].

The convergence of different technologies is one of the issues addressed by the subcommittees. The working group on IoT and Blockchain has already been cited from ISO/IEC JTC 1 subcommittee SC 41 or the document (under development) "Information Technology - Artificial Intelligence - Process Management Framework for Big Data Analytics" from ISO/IEC JTC 1 subcommittee SC 42.

As early as 2015[131] ENISA pointed to the lack of standardisation as one of the challenges in Big Data infrastructure and storage models. To which it adds the concern about the portability of security controls between different providers or even in Open-Source projects (such as Hadoop[132], for example).

In this regard, ENISA already called for standardisation in the document "Big Data Security"[133] of December 2015. Among the security recommendations is the following: "*Recommendation 4: Standardisation bodies should adapt existing security standards or create new standards for Big Data. Currently there are no specific certifications for Big Data, so standards will help the industry to move forward and provide better services to users.*" While ENISA acknowledges that there are no Big Data certifications, the same agency proposes to take as a starting point the list of Cloud Computing certifications, which is available today[134].

Interoperability is another concern of regulators. The US National Institute of Standards and Technology (NIST) has published its own interoperability framework: "The NIST Big Data Interoperability Framework (NBDIF)" with the aim of creating tools that can analyse data regardless of the platform on which it resides and that both data (Big Data) and analytics (Artificial Intelligence) can shift between platforms in an easy and agile way.

The European Commission has also addressed the issue of interoperability in the Communication "A European Data Strategy"*[135]*. Interoperability and data quality, as well as data structure, authenticity and integrity are key to exploiting the value of data, especially in the context of the deployment of Artificial Intelligence.

There are already specific ISO standards for IoT technologies:

- ISO 30141:2018: IoT Reference Architecture.
- ISO 20924:2018: IoT Vocabulary.

---

[130] IEC. Artificial intelligence across industries. International Electrotechnical Comission Whitepaper. https://basecamp.iec.ch/download/iec-white-paper-artificial-intelligence-across-industries-en/

[131] ENISA, Big Data Threat Landscape and Good Practice Guide, enero de 2016, https://www.enisa.europa.eu/publications/bigdata-threat-landscape

[132] N.B.: vid https://hadoop.apache.org

[133] ENISA, Big Data Security, op. cit.

[134] ENISA, "Cloud Computing Certification - CCSL and CCSM", https://resilience.enisa.europa.eu/cloud-computing-certification

[135] COMISIÓN EUROPEA, "Una Estrategia Europea de Datos", op. cit.

- ISO 21823-1:2019: IoT Interoperability (Part 1: Framework).
- ISO 22417:2017: IoT use cases.

Whereas in some of these standards there are some references to security and privacy (as in chapter 6.5.3 of ISA 28123: "Protection of personal data"; or chapter 11.4 of ISO 30141: "Personal data and information privacy") the ISO/IEC JTC 1/SC 27 subcommittee is developing the future ISO 27030 standard "Security and privacy guidelines for IoT" (currently under evaluation of the Working Draft by the Committee) which will establish a set of objectives, guidelines and controls to ensure the privacy and security of IoT environments.

NIST also has a reference document: NISTIR 8228: Considerations for Managing the Cyber Security and Privacy Risks of the Internet of Things (IoT)[136].

In order to solve or at least mitigate the interoperability and integration issues discussed above, a Data Governance framework, such as the one offered by DAMA, can be applied [137]. DAMA offers recommendations and best practices for eleven disciplines, one of them being interoperability and data integration.

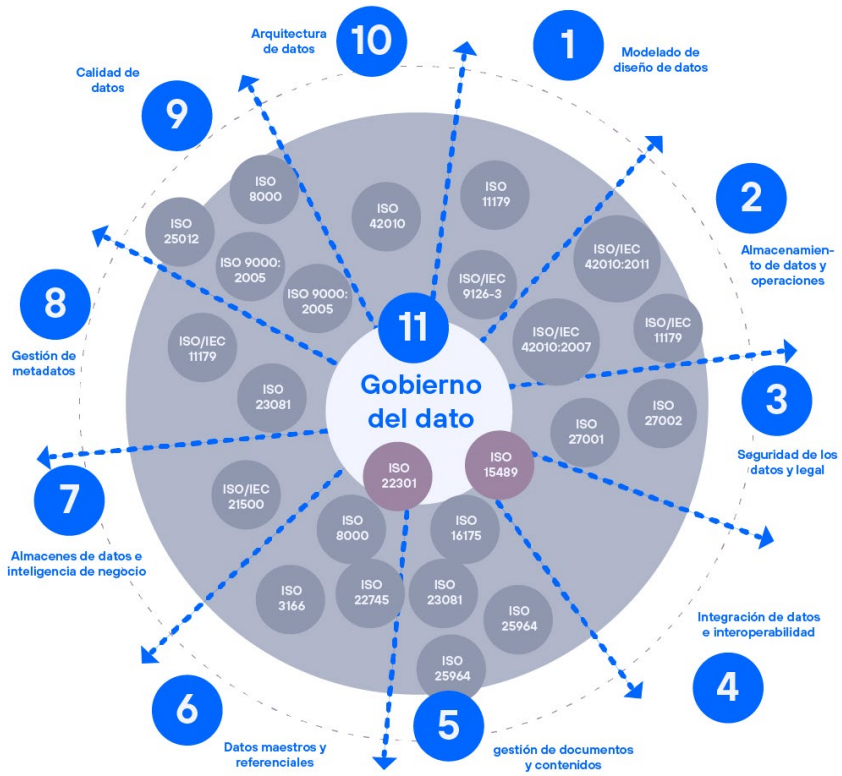


Image: ISOS applying to the DAMA disciplines of Data Governance.
SOURCE: DGU - Telefónica Tech IA of Things

[136] NIST, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks", *op. cit*.

[137] https://www.dama.org

3. Self-regulation through new certifications.

Carlos Manuel Fernández (IT Strategic Advisor at AENOR) and Boris Delgado Riss (ICT Manager at AENOR) believe that "*The advance and evolution of Information and Communication Technologies does not cease and its dizzying development is of such magnitude that the fourth industrial revolution and the Digital Transformation are having a profound impact on organisations, industries and society*". They refer to new technological scenarios such as SMAC (Social-Mobility-Analytics-Cloud), the development of the so-called Industry 4.0 (OT-Operation Technologies + IoT-Internet of Things), improvements in communication systems such as 5G and the advance of Artificial Intelligence and Machine Learning models. All of this, driven by data (Data-Driven), configures a scenario where new cyber threats and cyber risks arise in this Digital R-Evolution; and it is a revolution considering the continuous digital evolution.[138]

In this regard, AENOR has designed a Cyber Security and Privacy Ecosystem, based on international ISO standards/norms, as well as on current Spanish and European laws and regulations [139].

ENISA[140] refers to the need for stakeholders to invest in increasing the security skills of Big Data professionals through training and certification. The expected growth of Big Data in the coming years will require more qualified professionals, which will be linked to greater investment in training and certification to ensure secure Big Data environments.

CISOs, in addition to defining appropriate security measures, will need to align their systems with compliance with appropriate security standards. It will be crucial to have a joint vision of the interrelation of all the technologies involved: IoT, Artificial Intelligence, Big Data, etc.

The European Commission is proposing a system of risk assessment and voluntary pre or post monitoring for both IoT and Artificial Intelligence. Thanks to standardisation, the levels of risk involved in IoT technology for both security and privacy can be better defined. Audits can provide an answer to compliance in complex systems that bring together several technologies.

4. Self-regulation through ethics.

INITIATIVES

To address the situations discussed in the section on Ethical Impact, different organisations and companies have launched initiatives to ensure an ethical use of Artificial Intelligence that puts people first. An inventory of such initiatives can be found on the Algorithmwatch.org website[141] (a non-profit organisation whose aim is

[138] AENOR, "ISO/IEC 27001 y ENS, binomio perfecto para la ciberseguridad", por Boris Delgado Riss y Carlos Manuel Fernández, mayo de 2019.Online: <https://revista.aenor.com/348/isoiec-27001-y-ens-binomio-perfecto-para-la-ciberseguridad.html>.

[139] N.B.: vid https://www.aenorciberseguridad.com/certificacion1.html

[140] ENISA, Big Data Security..., op. cit.

[141] N.B.: vid. https://algorithmwatch.org/en/project/ai-ethics-guidelines-global-inventory/

to assess the social impact of AI), which includes public administrations, international organisations and manufacturers that want to demonstrate their concern.

One of the most important initiatives is the Ethical Guidance for Trusted Artificial Intelligence defined by the High-Level Expert Group on AI (HLEG [142]). This guide provides developers and Artificial Intelligence users with useful guidance through a series of principles and requirements [143]. The four guiding principles are respect for human autonomy, harm prevention, equity and explainability. The six requirements are human action and oversight, technical soundness and security, privacy and data management, transparency, diversity/non-discrimination, social welfare, and accountability[144].

The image below summarises the design framework for trusted AI in this guide, which takes into account the ethical impact of AI solutions:

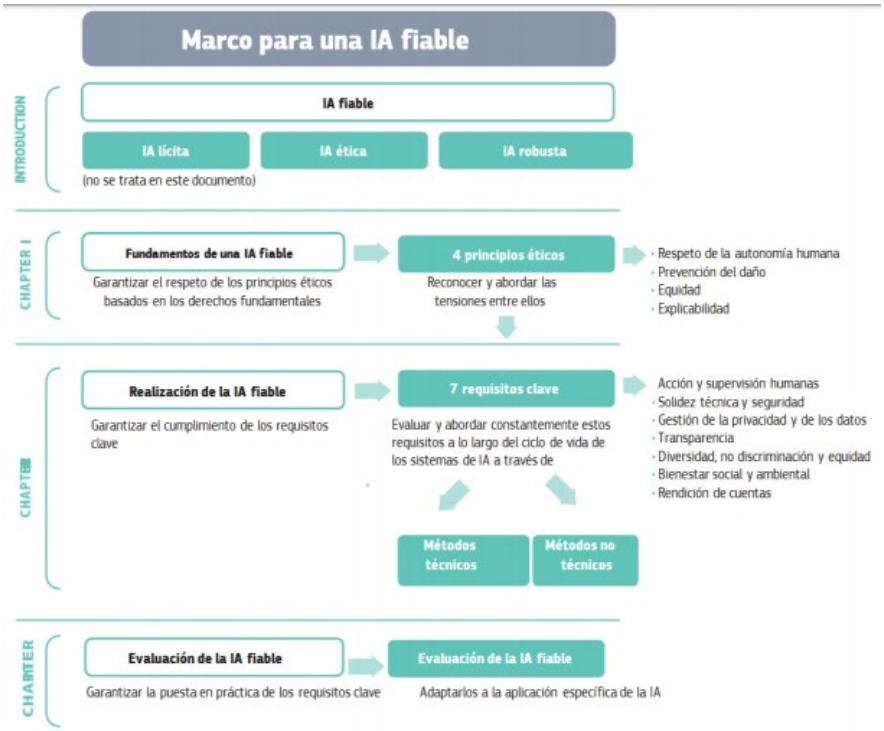


Image: EU AI ethical design framework.

[142] COMISIÓN EUROPEA, "High-Level Expert Group on Artificial Intelligence", https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

[143] COMISIÓN EUROPEA, Directrices éticas para una IA fiable..., op. cit.

[144] GOÑI SEIN, J.L., Defendiendo los derechos fundamentales frente a la Inteligencia Artificial, Universidad de Navarra, lección de 13 de septiembre de 2019, https://www.unavarra.es/digitalAssets/244/244921_100000Leccion-inaugural-Castellano-19-20_web.pdf

In Spain, the Artificial Intelligence strategy for R&D&I also includes, among its 6 priorities, the ethical analysis of AI applications so that they avoid several of the problematic situations seen and included in the EU Guide: avoiding negative biases and gender prejudices or other forms of discrimination, being aligned with ethical aspects or drafting an ethical code of AI in the coming years.

In September 2019, the OdiseIA[145] initiative also emerged in Spain, with the aim of creating a collaborative network of companies, organisations and individuals to serve as an observatory of the social and ethical impact of AI in our country.

Private companies such as Telefónica have also defined AI ethics as part of their social responsibility commitments [146]. The principles for the development of AI solutions and services are aligned with business principles, covering transparency, explainability, human rights, privacy or security.

In the same way, large technology companies such as Google[147], IBM[148], Facebook[149], or Microsoft[150] have publicly launched their commitment to follow ethical and responsible development principles.

CHALLENGES

While the problem is clearly defined (Artificial Intelligence, beyond the benefits it can bring, has ethical impacts that are very critical in people's lives) and companies and governments are launching multiple initiatives that show their commitment to address it, there is still some way to go to achieve a form of control similar to that which exists in the field of security and privacy..

On the one hand, there are no regulations and on the other hand, the way in which compliance can be audited by trusted third parties has not been determined. At the moment, their application depends mainly on the goodwill of companies and the level of awareness of users as a means of debate and pressure. In addition, ethical audits of algorithms are an essential part of contributing to the trustworthiness of AI solutions.

5. Social awareness

Data is the new oil, as it is metaphorically stated to highlight the increasing value attributed to it, the exploitation of which is dominated not only by the big five Western tech companies - Google, Amazon, Facebook, Apple and Microsoft (known by the acronym GAFAM) - but is something that has already led some

[145] N.B.: vid. online https://www.odiseia.org

[146] N.B.: vid. https://www.telefonica.com/es/web/negocio-responsable/nuestros-compromisos/principios-ia

[147] N.B.: vid. online https://ai.google/principles/

[148] N.B.: vid. online https://www.ibm.com/thought-leadership/institute-business-value/report/ai-ethics

[149] N.B.: vid. online https://ai.facebook.com/

[150] N.B.: vid. online https://www.microsoft.com/en-us/ai/responsible-ai?activetab=pivot1%3aprimaryr6

to talk about "the new cold war" when referring to the competition between China and the US for the development of AI, driven by Big Data and IoT.

The irruption of the capacity to exploit massive data is the milestone that marks a new before and after in our civilisational development. This is occurring in parallel to the highest elevation as a legal category of a cultural value of Western societies, privacy, which is not found in regimes like China or Russia[151]. This assumption, configured in our country as a fundamental right[152], has been the subject of extensive theoretical debate and - in practice - conditions, limits, undermines or even prevents the full implementation of Big Data projects.

One of the first conflicts revolves around the concept of trust [153]. What we consider reliable or unreliable - secure or insecure - varies according to our point of view. For example, the conflict of rights takes on a new perspective as the massive exploitation of data contributes to saving lives: thanks to Big Data, health data can now be said to be - metaphorically speaking - a true heritage of mankind[154]. The same could be said of Artificial Intelligence applications which, in the balance between the right to health and the right to data protection, weigh in favour of everything that is helping to combat the coronavirus pandemic.

On the other hand, from the point of view of regulatory systems, the change brought about by disruptive technologies entails a whole series of effects [155]: they provide solutions to regulatory problems by making some of the previous regulatory requirements unnecessary; they reveal existing legal loopholes; they challenge the modalities of regulatory control; they question the traditional powers of regulatory authorities; they cast doubt on the effectiveness of regulatory techniques... At the very least, while offering great expectations of social and economic benefit, they hold the great uncertainty of potential costs.

Two recent surveys: the first by Eurobarometer, conducted in March 2019 - just one year after the entry into force of the European Data Protection Regulation - and the second by the Spanish Sociological Research Centre, conducted in May 2018 on a variety of issues, devote an extensive section to the perception of personal data protection.

In general terms, the issue that most concerns Spaniards is the protection of personal data and the possible use of personal information by other people, with a clear difference with respect to the other two issues that follow: advances in science and technology or the development of communication and information via the Internet.

---

[151] CRAIG, T., LUDLOFF, M. E., *Privacy and Big Data*, O'Reilly, Sebastopol (CA), 2011, págs. 19-20.

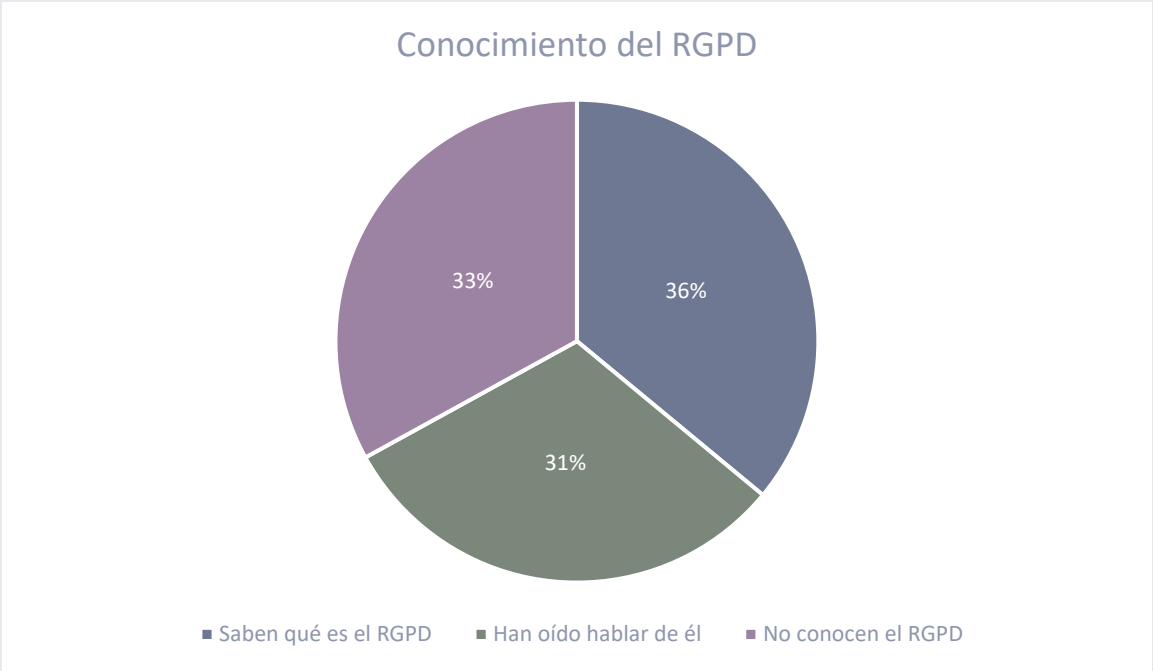
[152] **N.B.:** *Artículo 18.4 de la Constitución Española de 1978, en relación con las Sentencias del Tribunal Constitucional números 290 y 292, de 30 de noviembre de 2000.*

[153] SCHNEIER, B., "Technologists vs. Policy Makers", *IEEE Security & Privacy*, vol. 18, January-February 2020, págs. 71-72.

[154] DE MONTALVO JÄÄSKELÄINEN, F., *op. cit.*

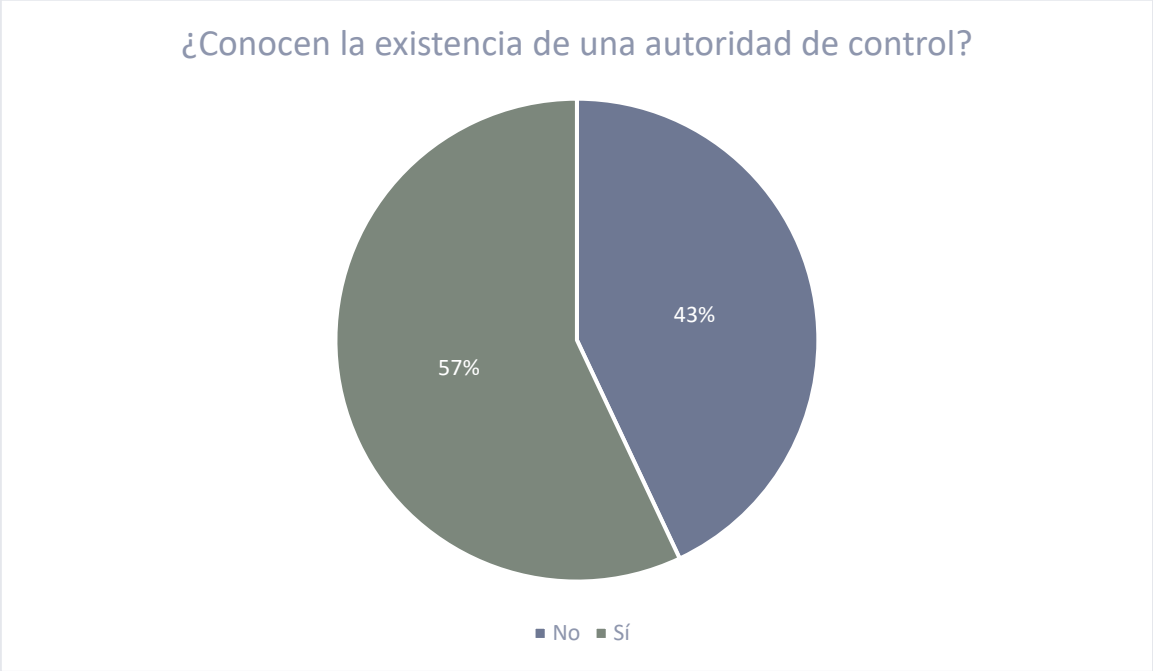
[155] MASHAW, J. L., "Prólogo", en: Recuerda Girela, M. A., *Tecnologías disruptivas: Regulando el futuro*, Aranzadi, Pamplona, págs. 41-43.

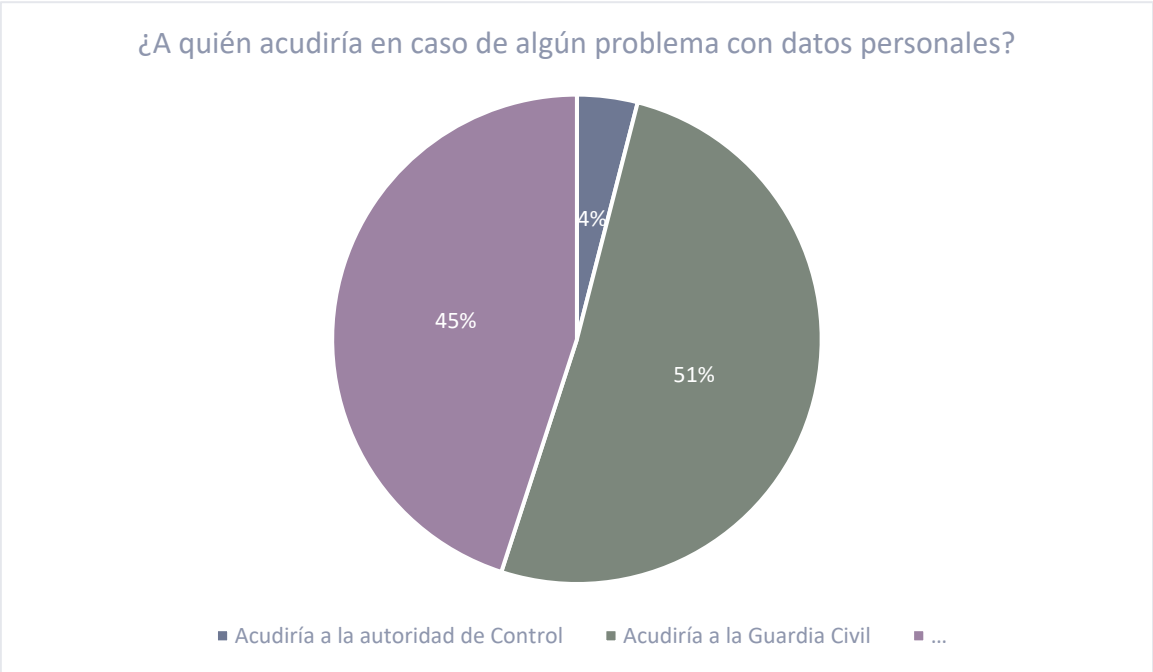
However, with regard to knowledge about the rules protecting this essential sphere of individuals, at European level the results[156] indicate that respondents are relatively well aware of the new data protection rules, their rights and the existence of national data protection authorities, to whom they can turn for help in case of a violation of their rights. This is reflected in the fact that 67% are aware of the existence of the GDPR, although only 36% of these know what the Regulation is, while 31% have heard of it but do not know exactly what it is.



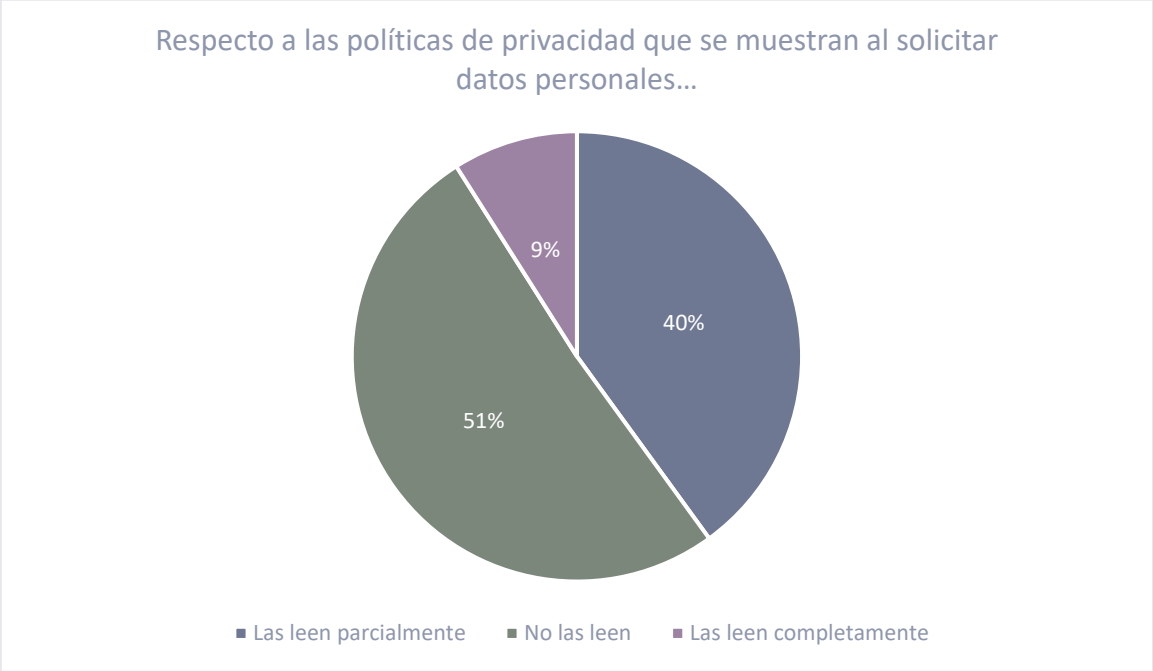
In this context, around six out of ten Europeans (57%) say they have heard something about the existence of a public authority in their country responsible for protecting their rights regarding their personal data. Even so, according to CIS data (2018) only 4% of Spaniards would first turn to this authority in the event of suffering any kind of problem with their personal data, while 51% would first turn to the Police or Guardia Civil.

[156] Todos los resultados que se citan del Eurobarómetro han sido consultado y extraídos de: COMISIÓN EUROPEA, "487a. General Data Protection Regulation - 487b. Charter of Fundamental Rights", Public Opinion, marzo de 2019, https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222





In the Spanish case, with regard to the privacy policies shown when requesting personal data on the Internet, only 9% of Internet users admit to reading them completely, while 40% say they read them partially, which means that half of Spanish Internet users do not read any of these sections and privacy statements.



Another relevant aspect would be why internet users do not read these privacy policies: the main reason in all EU countries is that they are too long, with the second most commonly cited reason (as in the case of Spain) being that they are unclear or difficult to understand - a perception shared by 70% of those interviewed by the CIS.

Given this data, it could be argued that citizens are clearly concerned about their privacy, but it is particularly revealing that some people are already trying to understand how their personal data is processed and to act accordingly.

Awareness campaigns launched by institutions and agencies represent a strong point for the alliance between users and the system.

At EU level, the European Commission encourages users to read privacy statements and optimise their privacy choices by organising a section on its website dedicated to frequently asked questions and providing easy and understandable answers.

Several initiatives can also be found in Spain. Firstly, the National Cybersecurity Institute launches awareness campaigns[157] that explain in a simple way issues related to social networks, devices used at work, mobiles, online shopping, password configuration... using infographics or videos. In addition, the Spanish Data Protection Agency stands out for its informative work through the publication of numerous Guidelines. In this

[157] N.B.: vid. https://www.osi.es/es/campanas

case, the Citizen's Guidelines[158] are an example of the SDPA's willingness to guide and enlighten not only private entities or organisations but also the general population.

Google and the Consumers and Users Organisation, in collaboration with the SDPA and the National Institute of Cybersecurity, have announced the launch of the second edition of their *Vive un Internet seguro* campaign, which aims to continue informing Internet users and giving them the necessary tools to ensure their protection in terms of privacy and security on the Internet, by providing a free and accessible platform[159] where they can find a guide for parents and educators, advice, tests, etc.

In the autonomous community context, the *Generalitat Valenciana* has also shown its commitment to raising awareness by drawing up, from the Data Protection Delegation, some recommendations, among which we can highlight the one relating to the exercise of the right of access[160]. Likewise, the *Centre de Seguretat TIC de la Comunitat Valenciana* has created the *ConcienciaT* platform, where you can find a wide variety of infographics on how to maintain security in different areas: tourism, health environments, use of IoT devices, etc.

For this reason, only users, with the tools and knowledge necessary to know what their data is being used for, can be an active part of this relationship with entities and administrations that process their data, which, for their part, must contribute by applying due transparency in their practices and respecting the appropriate ethical, legal and security standards from the design and by default.

[158] AEPD, Protección de Datos: Guía para el Ciudadano, mayo de 2020, https://www.aepd.es/sites/default/files/2020-05/guia-ciudadano.pdf

[159] N.B.: vid. https://viveinternetseguro.org/?_ga=2.118806153.149690011.1569926083-363139414.1569926083

[160] GENERALITAT VALENCIANA, "Recomendación Ejercicio del Derecho de Acceso", Delegación de Protección de Datos GVA, 2019, http://participacio.gva.es/documents/166475129/167697765/Recomendaci%C3%B3n+2019%20001.+Ejercicio+del+Derecho+de+Acceso.pdf/ee4ed75c-196e-4366-9619-4a66c09e9662

Bibliography

AENOR, "ISO/IEC 27001 y ENS, binomio perfecto para la ciberseguridad", por Boris Delgado Riss y Carlos Manuel Fernández, mayo de 2019.Online: <https://revista.aenor.com/348/isoiec-27001-y-ens-binomio-perfecto-para-la-ciberseguridad.html>.

AEPD, *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*, 2020, p. 5. Online: <https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf>.

AEPD, *Código de buenas prácticas en protección de datos para proyectos Big Data*, Coords.: Emilio Aced, M. Rosario Heras y Carlos Alberto Sáiz, 2019, pág 3. Online: <https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf>.

AEPD, *Protección de Datos: Guía para el Ciudadano*, mayo de 2020. Online: <https://www.aepd.es/sites/default/files/2020-05/guia-ciudadano.pdf>.

APDCAT, *Inteligencia Artificial: Decisiones Automatizadas en Cataluña*, 2020, pág. 21. Online: <https://apdcat.gencat.cat/web/.content/04-actualitat/noticies/documents/Informe-IA-Castellano.pdf>.

BARRIO, M., *Internet de las Cosas*. Madrid: Reus, 2018, pág. 21.

BEJERANO, P., "Diferencias entre machine learning y deep learning", *Telefónica Think Big Empresas*, 8 de febrero de 2017. Online: <https://blogthinkbig.com/diferencias-entre-machine-learning-y-deep-learning>.

CAPGEMINI RESEARCH INSTITUTE, "Reinventing Cybersecurity With Artificial Intelligence", 2019. Online: <https://www.capgemini.com/es-es/wp-content/uploads/sites/16/2019/07/AI-in-Cybersecurity_Report_20190710_V05.pdf>.

CEPAL, Informe "La Nueva Revolución Digital: de la Internet del consumo a la Internet de la producción". Comisión Económica para América Latina y el Caribe, 2018, p. 36. Online: <https://repositorio.cepal.org/bitstream/handle/11362/38604/4/S1600780_es.pdf>.

CESE, "Inteligencia artificial: anticipar su impacto en el trabajo para garantizar una transición justa", Dictamen 2018/C 440/0, Comité Económico y Social Europeo, 6 de diciembre de 2018, p. 3.

CIS, *Barómetro de mayo de 2018*, estudio nº 3213. Online: <http://datos.cis.es/pdf/Es3213mar_A.pdf>.

COMISIÓN EUROPEA, *A Definition of AI: Main capabilities and disciplines,* por el grupo de expertos de alto nivel en Inteligencia Artificial, 2018, pág. 6. Online: <https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>.

COMISIÓN EUROPEA , *"El momento de Europa: reparar los daños y preparar el futuro para la próxima generación",* Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM(2020) 456 final, Online: <https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2020/0456/COM_COM(2020)0456_ES.pdf>.

COMISIÓN EUROPEA, *Directrices éticas para una IA fiable,* Grupo de expertos de alto nivel en Inteligencia Artificial, abril de 2019. Online: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.

COMISIÓN EUROPEA, "Hacia una economía de los datos próspera", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM/2014/0442 final, 2 de julio de 2014. Online: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52014DC0442&from=ES>.

COMISIÓN EUROPEA, "High-Level Expert Group on Artificial Intelligence", Online: <https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence>.

COMISIÓN EUROPEA, "La construcción de una economía de los datos europea", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM (2017) 9 final, 10 de enero de 2017.

COMISIÓN EUROPEA, *Libro Blanco sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza*, COM(2020) 65 final, 19 de febrero de 2020. Online: <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf>.

COMISIÓN EUROPEA, "Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica", Informe a la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones, COM(2020) 64 final, 19 de febrero 2020. Online: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0064>.

COMISIÓN EUROPEA, "Inteligencia artificial para Europa", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM(2018) 237 final, 25 de abril de 2018. Online: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/ES/COM-2018-237-F1-ES-MAIN-PART-1.PDF>.

COMISIÓN EUROPEA, Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de Seguridad Aérea de la Unión Europea, y se deroga el Reglamento (CE) nº 216/2008 del Parlamento Europeo y del Consejo, 2015/0277/COD, 7 de diciembre de 2015, artículo 3 (29).

COMISIÓN EUROPEA, *Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre* el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), 2017/0003(COD), 10 de enero de 2017. Online:

COMISIÓN EUROPEA, "Una Estrategia Europea de Datos", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR , COM(2020) 66 final, 19 de febrero de 2020. Online: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0066&from=ES>.

COMISIÓN EUROPEA, "Una Estrategia para el Mercado Único Digital de Europa", Comunicación al Parlamento Europeo, al Consejo, al CESE y CDR, COM(2015) 192 final, 6 de mayo de 2015. Online: < https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52015DC0192&from=ES>.

COTINO HUESO, L., "Riesgos e impactos del Big Data, la Inteligencia Artificial y la robótica. Enfoques, modelos y principios de la respuesta del Derecho", *Revista General de Derecho Administrativo*, nº50, 2019, p.7.

COMISIÓN EUROPEA, "487ª. General Data Protection Regulation - 487b. Charter of Fundamental Rights", *Public Opinion*, marzo de 2019. Online: <https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instru ments/special/surveyky/2222>.

CONSEJO DE EUROPA, "Algorithms and human rights - Study on the human rights dimensions of automated data processing techniques and possible regulatory implications", Committee of experts on internet intermediaries (MSI-NET), 2018. Online: <https://edoc.coe.int/en/internet/7589-algorithms-and-human-rights-study-on-the-human-rights-dimensions-of-automated-data-processing-techniques-and-possible-regulatory-implications.html>.

CONSEJO DE EUROPA, Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, Roma, 4 de noviembre de 1950.

CRAIG, T., LUDLOFF, M. E., *Privacy and Big Data*, O'Reilly, Sebastopol (CA), 2011

DGT, "Instrucción 15/V-113 sobre autorización de pruebas o ensayos de investigación realizados con vehículos de conducción automatizada en vías abiertas al tráfico en general", Dirección General de Tráfico del Ministerio del Interior, p. 1. Online: <http://www.dgt.es/Galerias/seguridad-vial/normativa-legislacion/otras-normas/modificaciones/15.V-113-Vehiculos-Conduccion-automatizada.pdf>.

DGT, "Instrucción 16 TV/89 sobre estacionamiento asistido de vehículos a motor", Dirección General de Tráfico del Ministerio del Interior, 20 de enero de 2016. Online: <http://www.dgt.es/Galerias/seguridad-vial/normativa-legislacion/otras-normas/modificaciones/2016/Instruccion_16_TV_89_Estacionamiento_asistido_vehiculos_motor. pdf>.

EL PAÍS, "Amazon prescinde de una inteligencia artificial de reclutamiento por discriminar a las mujeres", por Isabel Rubio, 12 de octubre de 2018. Online: <https://elpais.com/tecnologia/2018/10/11/actualidad/1539278884_487716.html>.

ENISA, *Big Data Security Good Practices and Recommendations on the Security of Big Data Systems*, diciembre de 2015. Online: <https://www.enisa.europa.eu/publications/big-data-security>.

ENISA, *Big Data Threat Landscape and Good Practice Guide*, enero de 2016. Online: <https://www.enisa.europa.eu/publications/bigdata-threat-landscape>.

ENISA, "Cloud Computing Certification - CCSL and CCSM". Online: <https://resilience.enisa.europa.eu/cloud-computing-certification>.

ESPAÑA, Constitución Española, BOE 29 de diciembre de 1978, artículo 55.

GENERALITAT VALENCIANA, "Recomendación Ejercicio del Derecho de Acceso", Delegación de Protección de Datos GVA, 2019. Online: <http://participacio.gva.es/documents/166475129/167697765/Recomendaci%C3%B3n+2019%2 0001. +Ejercicio+del+Derecho+de+Acceso.pdf/ee4ed75c-196e-4366-9619-4a66c09e9662>.

GOBIERNO DE ESPAÑA, *Estrategia Española de I+D+i en Inteligencia Artificial*, Ministerio de Ciencia, Innovación y Universidades, 2019. Online: <https://www.ciencia.gob.es/stfls/MICINN/Ciencia/Ficheros/Estrategia_Inteligencia_Artificial_I DI.pdf>.

GOÑI SEIN, J.L., *Defendiendo los derechos fundamentales frente a la Inteligencia Artificial*, Universidad de Navarra, lección de 13 de septiembre de 2019. Online: <https://www.unavarra.es/digitalAssets/244/244921_100000Leccion-inaugural-Castellano-19-20_web.pdf>.

GT29, *Dictamen 8/2014 sobre la evolución reciente del Internet de los Objetos,* elaborado por el Grupo de Trabajo sobre protección de datos del artículo 29 (Unión Europea), 16 septiembre de 2014, pág. 4. Online: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_es.pdf>.

GUADAMUZ, A., "La inteligencia artificial y el derecho de autor", OMPI revista, octubre de 2017. Online: <https://www.wipo.int/wipo_magazine/es/2017/05/article_0003.html>.

HOFFMANN-RIEM, W., *Big Data. Desafíos también para el Derecho*, Pamplona: Civitas, 2018, pág. 51.

IEC. *Artificial intelligence across industries*. International Electrotechnical Comission Whitepaper. Online: <https://basecamp.iec.ch/download/iec-white-paper-artificial-intelligence-across-industries-en/>.

IEC, "ISO/IEC JTC 1/SC 41 Work programme". Online: <https://www.iec.ch/dyn/www/f?p=103:23:8187723854992::::FSP_ORG_ID,FSP_LANG_ID:20486 ,25>.

IDC RESEARCH ESPAÑA, "El Mercado de Internet de las Cosas en España". Online: <https://idcspain.com/research/IoTSpain>.

IMREI, K. (Ed.), "Data as the Engine of Europe's Digital Future", *The European Data Market Monitoring Tool Report*, junio de 2019, 51 págs. Online: <http://datalandscape.eu/sites/default/files/report/EDM_D2.5_Second_Report_on_Policy_Conclusions_final_13.06.2019.pdfZ>.

IoT ANALYTICS, *IoT Platforms Company Landscape 2020*. Online: <https://iot-analytics.com/product/iot-platforms-landscape-database-2020>.

ISO, "ISO/IEC JTC 1Information Technology", International Organization for Standardization. Online: <https://www.iso.org/isoiec-jtc-1.html>.

JUANES, C., DE FUENTES, J.M., SAN JOSÉ, J., "Ciberseguridad: Inteligencia artificial para garantizar la mejor defensa", *Marketing y Ventas*, núm. 161, mayo de 2020.

KALYANI, V.L., SHRAMA., D., "IoT: Machine to Machine (M2M), Device to Device (D2D) Internet of Everything (IoE) and Human to Human (H2H): Future of Communication", *JMEIT*, v. 2, nº. 6, diciembre de 2015. Online:

<http://www.jmeit.com/JMEIT%20Vol%202%20Issue%206%20Dec%202015/JMEITDEC02060 03.pdf>.

LANEY, D., "3D Data Management: Controlling Data Volume, Velocity, and Variety", *Application Delivery Strategies*, META Group Inc, fichero 949, 6 de febrero de 2001, Online: <https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>.

LOZA CORERA, M., "Big data e inteligencia artificial", *Govertis Advisory Services*, 4 de diciembre 2018. Online: <https://www.govertis.com/big-data-e-inteligencia-artificial>.

LOZA CORERA, M., "Hacia la economía de los datos europea: nuevo reglamento europeo 2018/1807", *Govertis Advisory Services*, 10 de diciembre de 2018. Online: <https://www.govertis.com/hacia-la-economia-de-los-datos-europea-nuevo-reglamento-europeo-2018-1807#_ftn3>.

LUCA, "¿Qué es la Inteligencia Artificial?", Diccionario Tecnológico. Online: <https://luca-d3.com/es/data-speaks/diccionario-tecnologico/inteligencia-artificial>.

MASHAW, J. L., "Prólogo", en: Recuerda Girela, M. A., *Tecnologías disruptivas: Regulando el futuro*, Aranzadi, Pamplona, págs. 41-43.

MAYER-SCHÖNBERGER, V., CUKIER, K., *Big data. La revolución de los datos masivos*, Madrid: Turner, 2013, pág. 22.

MERCADER UGUINA, J. R., "El futuro del trabajo y el empleo en la era de la digitalización y la robótica", En: DE LA QUADRA-SALCEDO, T., PIÑAR MAÑANAS, J. L. (Dirs.), Sociedad digital y Derecho, Madrid: BOE, 2018, pág. 617. Online: <https://www.boe.es/publicaciones/biblioteca_juridica/abrir_pdf.php?id=PUB-NT-2018-97>.

NACIONES UNIDAS, Declaración Universal de los Derechos Humanos, 217 (III) A. Paris, 1948.

NACIONES UNIDAS, *Pacto Internacional de Derechos Civiles y Políticos*. Resolución 2200 A (XXI) de la Asamblea General, 16 de diciembre de 1966.

NIST, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks", NISTIR 8228, junio de 2019. Online: <https://csrc.nist.gov/publications/detail/nistir/8228/final>.

PARLAMENTO EUROPEO, "El mercado único digital omnipresente", Fichas temáticas sobre la Unión Europea Parlamento Europeo. Online: <https://www.europarl.europa.eu/factsheets/es/sheet/43/el-mercado-unico-digital-omnipresente>.

PARLAMENTO EUROPEO, Resolución del Parlamento Europeo, de 12 de septiembre de 2018, sobre los sistemas armamentísticos autónomos. Online: <https://www.europarl.europa.eu/doceo/document/TA-8-2018-0341_ES.html>.

PÉREZ, C., "Aspectos legales del Big Data", *Revista de Estadística y Sociedad*, nº 68, 2016, p. 18.

PURDY. M, DAUGHERTY, P., Informe "Inteligencia Artificial, el futuro del crecimiento", *Accenture*, 2016, p. 4. Online: <https://www.accenture.com/cl-es/insight-artificial-intelligence-future-growth>.

PWC IDEAS, "Inteligencia artificial y Blockchain, el yin y el yang de la tecnología", 2016. Online: <https://ideas.pwc.es/archivos/20161111/inteligencia-artificial-y-blockchain-el-yin-y-el-yang-de-la-tecnologia>.

RABAH, K., "Convergence of AI, IoT, Big Data and Blockchain: A Review", *The Lake Institute Journal*, vol.1, núm.1, 2018, págs. 1-18.

RECUERO DE LOS SANTOS, P., "Tipos de aprendizaje en Machine Learning: supervisado y no supervisado", *Telefónica Think Big Empresas*, 16 de noviembre de 2017. Online: <https://empresas.blogthinkbig.com/que-algoritmo-elegir-en-ml-aprendizaje>.

RICHARDSON, R., SCHULTZ, J., CRAWFORD, K., "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice," *94 N.Y.U. L. Rev. Online,* nº 192, marzo 2019. Online: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333423>.

RODRÍGUEZ CANFRANC, P. et al., "Sociedad Digital en España 2019", *Fundación Telefónica*, abril 2020, pág. 28. Online: <https://www.fundaciontelefonica.com/noticias/informe-sociedad-digital-espana-2019>.

SAMOILI, S., LÓPEZ COBO, M., GÓMEZ, E., DE PRATO, G., MARTÍNEZ-PLUMED, F., & DELIPETREV, B., *AI Watch. Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence*, Luxembourg: Publications Office of the European Union, 2020, pág. 8. Online: <https://ec.europa.eu/jrc/en/publication/ai-watch-defining-artificial-intelligence>.

SÁNCHEZ CHINCHÓN, A., "Los algoritmos nos facilitan la vida: así funcionan", *Telefónica Think Big Empresas,* 21 de noviembre de 2016. Online: <https://empresas.blogthinkbig.com/los-algoritmos-nos-facilitan-la-vida-asi-funcionan>.

SANTAMARÍA RAMOS, F. J.: "Internet de las cosas: un desafío para la protección de datos personales", Actualidad Administrativa nº 7-8, julio-agosto 2015, págs. 40-57.

SCHNEIER, B., "Technologists vs. Policy Makers", *IEEE Security & Privacy*, vol. 18, January-February 2020, págs. 71-72.

THE GUARDIAN, "Rise of the racist robots – how AI is learning all our worst impulses", por Stephen Buranyi, 8 de agosto de 2017. Online:

<https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses>

THE GUARDIAN, "The great British Brexit robbery: how our democracy was hijacked", por Carole Cadwalladr, 7 de mayo de 2017. Online: <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy>.

TRIBUNAL CONSTITUCIONAL, Sentencia 24/2019, de 25 de febrero, FJ 5. Online: <http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/25869#complete_resolucion&fund amentos>.

TRIBUNAL CONSTITUCIONAL, Declaración inconstitucionalidad artículo 58bis LOPDGDD, vid. SENTENCIA 76/2019, de 22 de mayo. Online: <https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_076/2019-1405STC.pdf>.

TSCHIDER, Ch., "Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence", *96 Denv. U. L. Rev. 87 Age*, marzo de 2018, pág. 120.

UNE, "Impulso español a las normas mundiales sobre IA, Big Data e IoT", por José Antonio Jiménez, *La revista de la normalización española*, enero de 2020. Online: <https://revista.une.org/21/impulso-espanol-a-las-normas-mundiales-sobre-ia-big-data-e-i.html>.

WEF, "COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications", 2020. Online: <https://www.weforum.org/global-risks/reports>.

About Telefónica Tech

Telefónica Tech is a key holding of the Telefónica Group. The company offers a wide range of integrated technology services, reaching more than 5.5 million customers in 175 countries every day. Telefonica TECH will host other digital businesses in the future, including in the B2C segment.

More information

telefonicatech.com