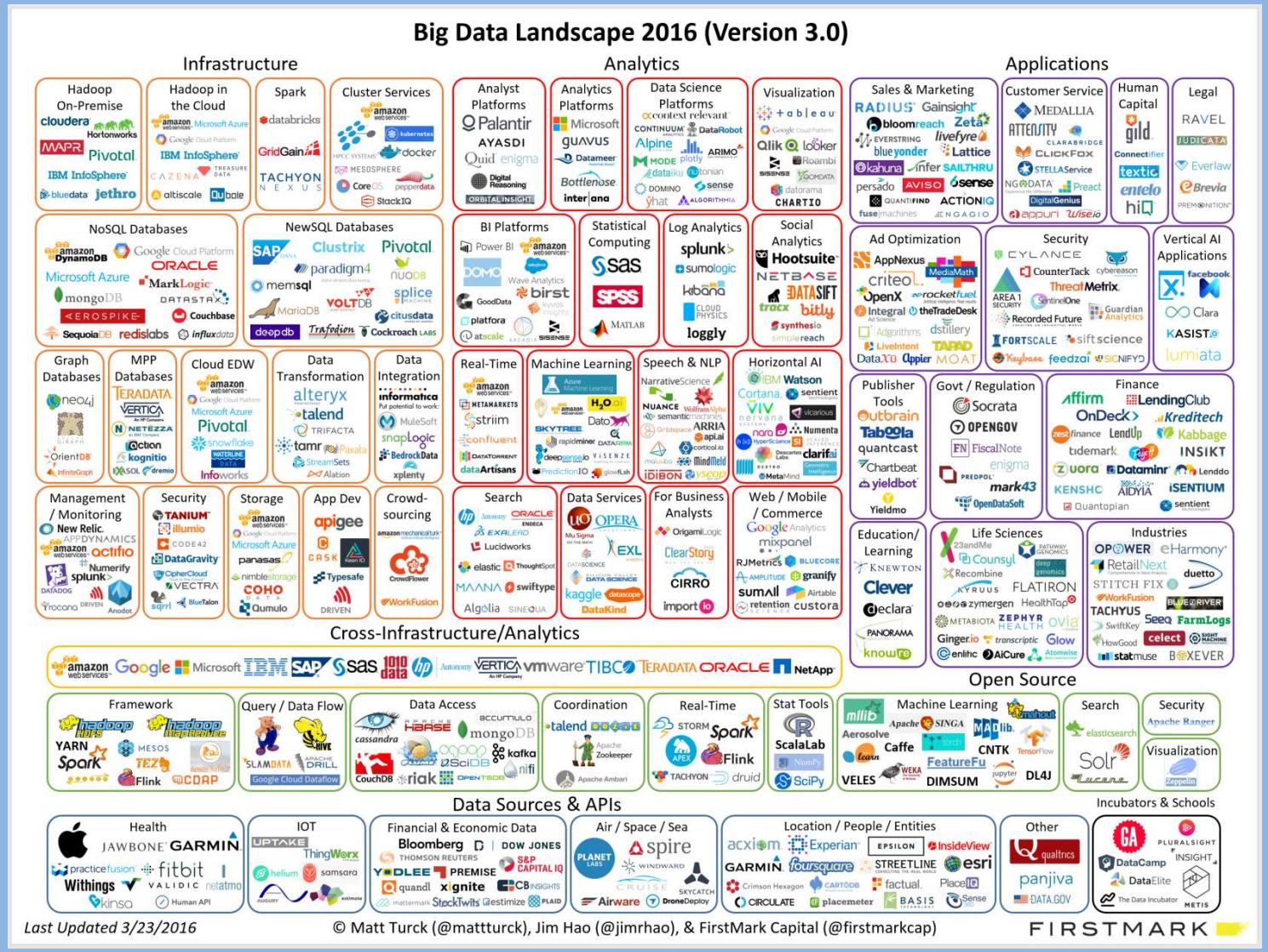
BIG DATA Y PROTECCIÓN DE DATOS PERSONALES

1 de junio de 2022

Cecilia Alvarez Rigaudias

¿QUÉ ES BIG DATA?

2016



http://mattturck.com/wp-content/uploads/2017/03/Big-Data-Landscape-2017-v18-FINAL.png

¿QUÉ ES BIG DATA?

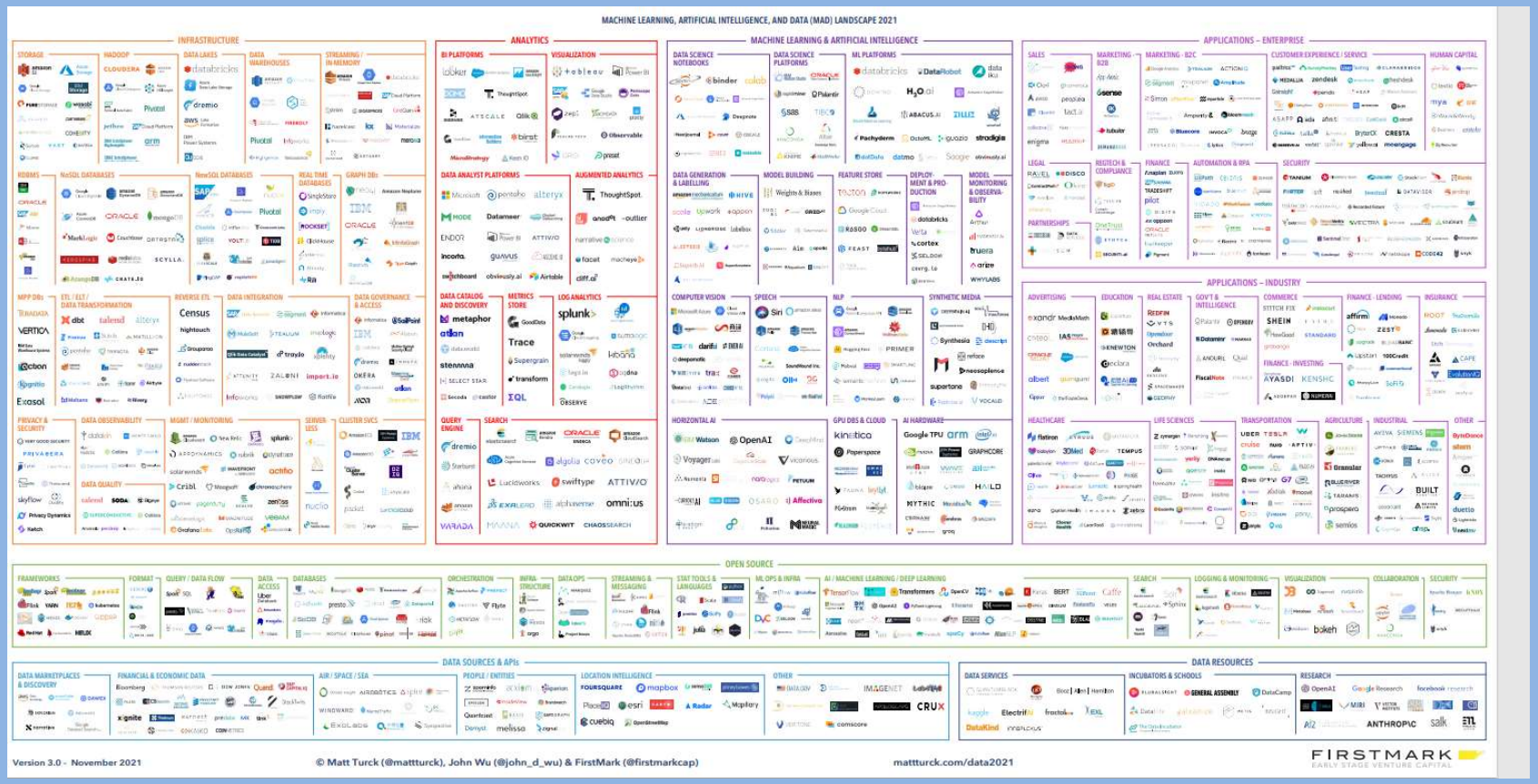
2018

2021

[The State of Data Engineering in 2022 | RudderStack Blog]

¿QUÉ ES BIG DATA?

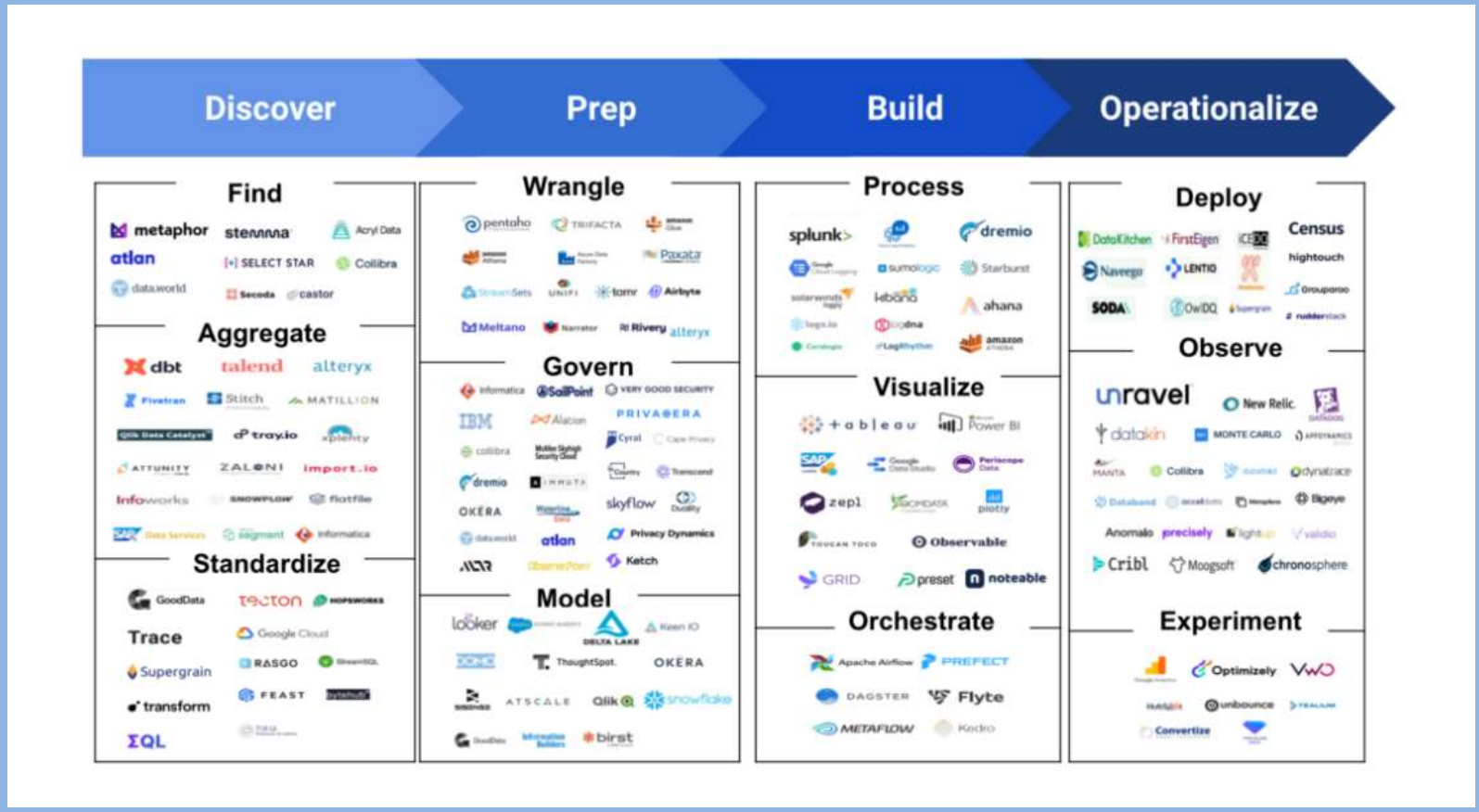
2021



[Artboard 1 (netdna-ssl.com)]

¿QUÉ ES BIG DATA?

2022



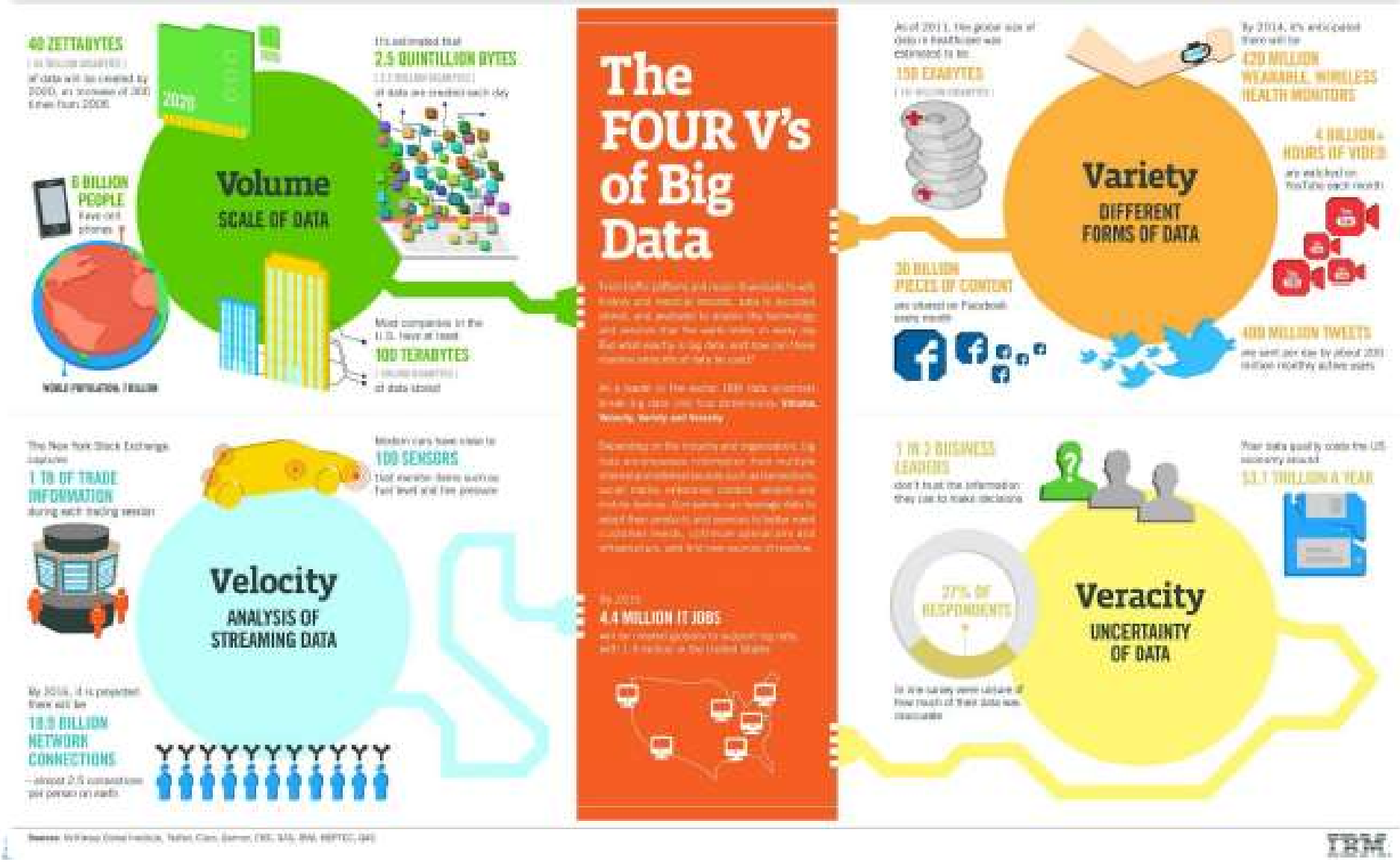
http://mattturck.com/wp-content/uploads/2017/03/Big-Data-Landscape-2017-v18-FINAL.png

¿QUÉ ES BIG DATA?

2022

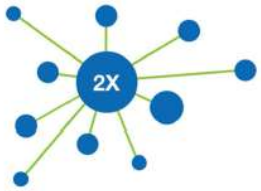
Leading lawmakers gathered at the Hannover Messe this week. In his speech yesterday, Thierry Breton said *"big data is the new fuel that will power tomorrow's industry, benefiting businesses, consumers, public services and society as a whole. But for this to happen, Europe needs to grow stronger in sharing and exploiting industrial data. That is the objective of the legislative proposals on data, and of our work to promote common European data spaces."* Robert Habeck, German Minister for economic affairs and climate action, also agreed that there's a need for *"highly interoperable industry data spaces"* to further digitise European industry.

DEFINICIÓN DE BIG DATA



https://www-01.ibm.com/software/data/bigdata/

DEFINICIÓN DE BIG DATA



The Data Explosion

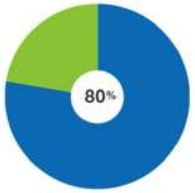
Medical data is expected to double every 73 days by 2020.

A Quick Study

Watson can read 40 million documents in 15 seconds.

https://www.ibm.com/watson/health/

IBM Watson



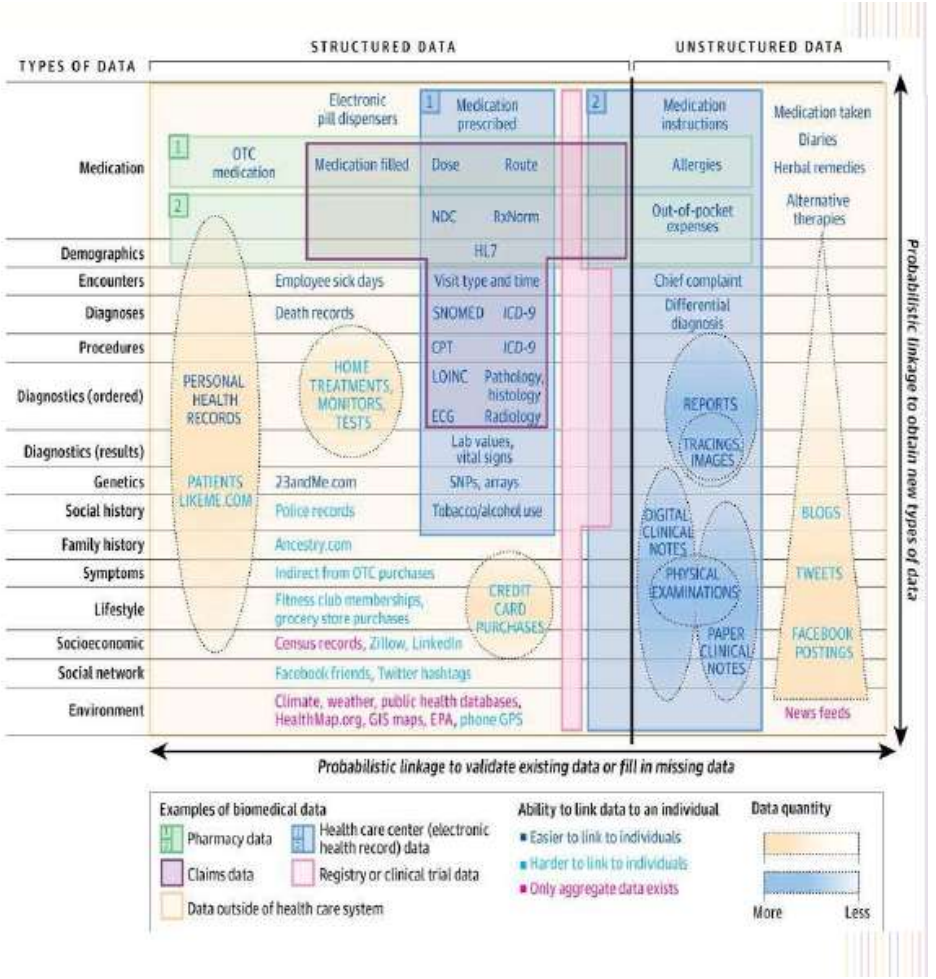
The Great Unknown

80% of health data is invisible to current systems because it's unstructured. Watson Health can see it.

21.3.2017

Prof. Dr. C. Woopen

Slide 10

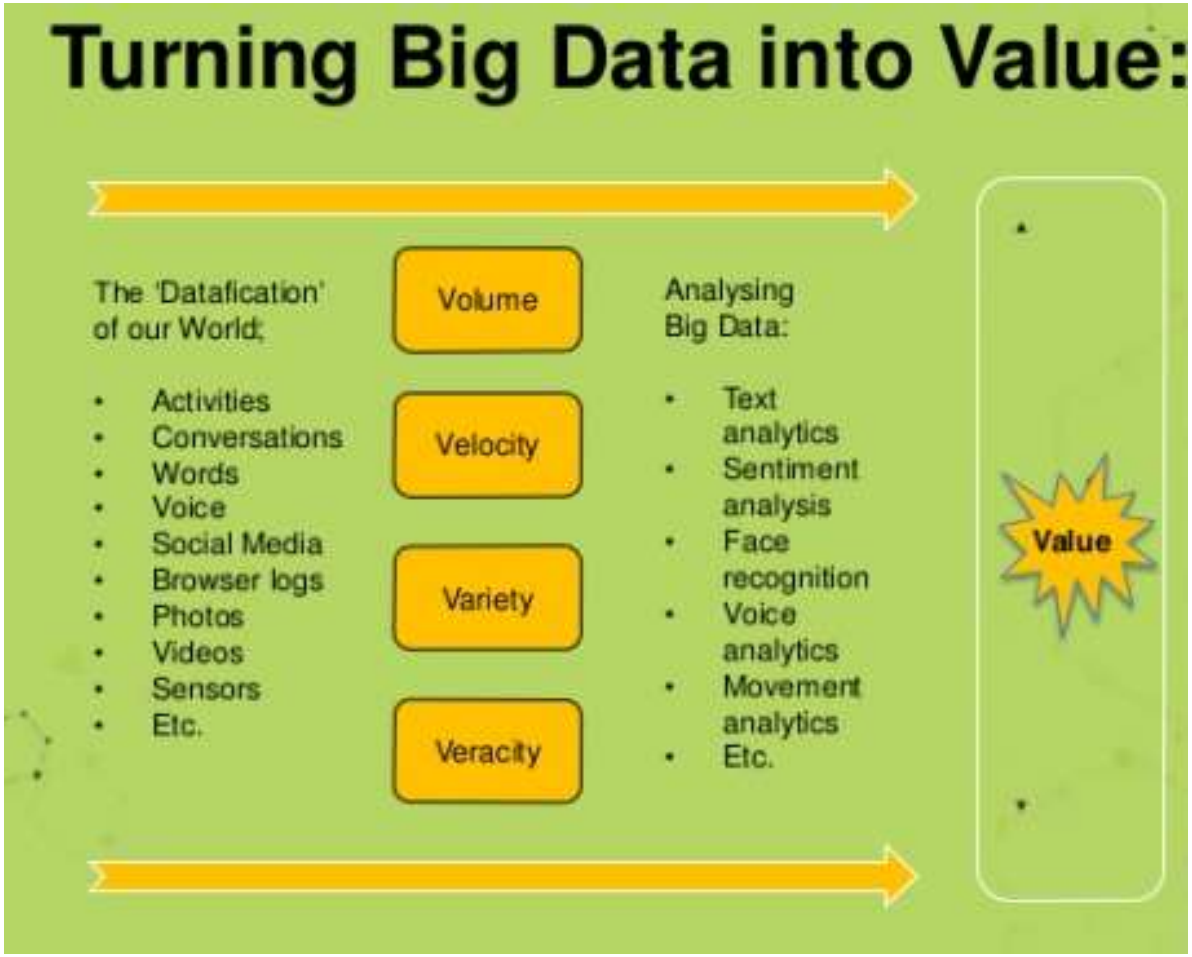


http://www.msssi.gob.es/estadEstudios/estadisticas/sisInfSanSNS/foroSistemaInfoSNS/ponencias_Big_Data/BIGDATA_1M_3Woopen.pdf

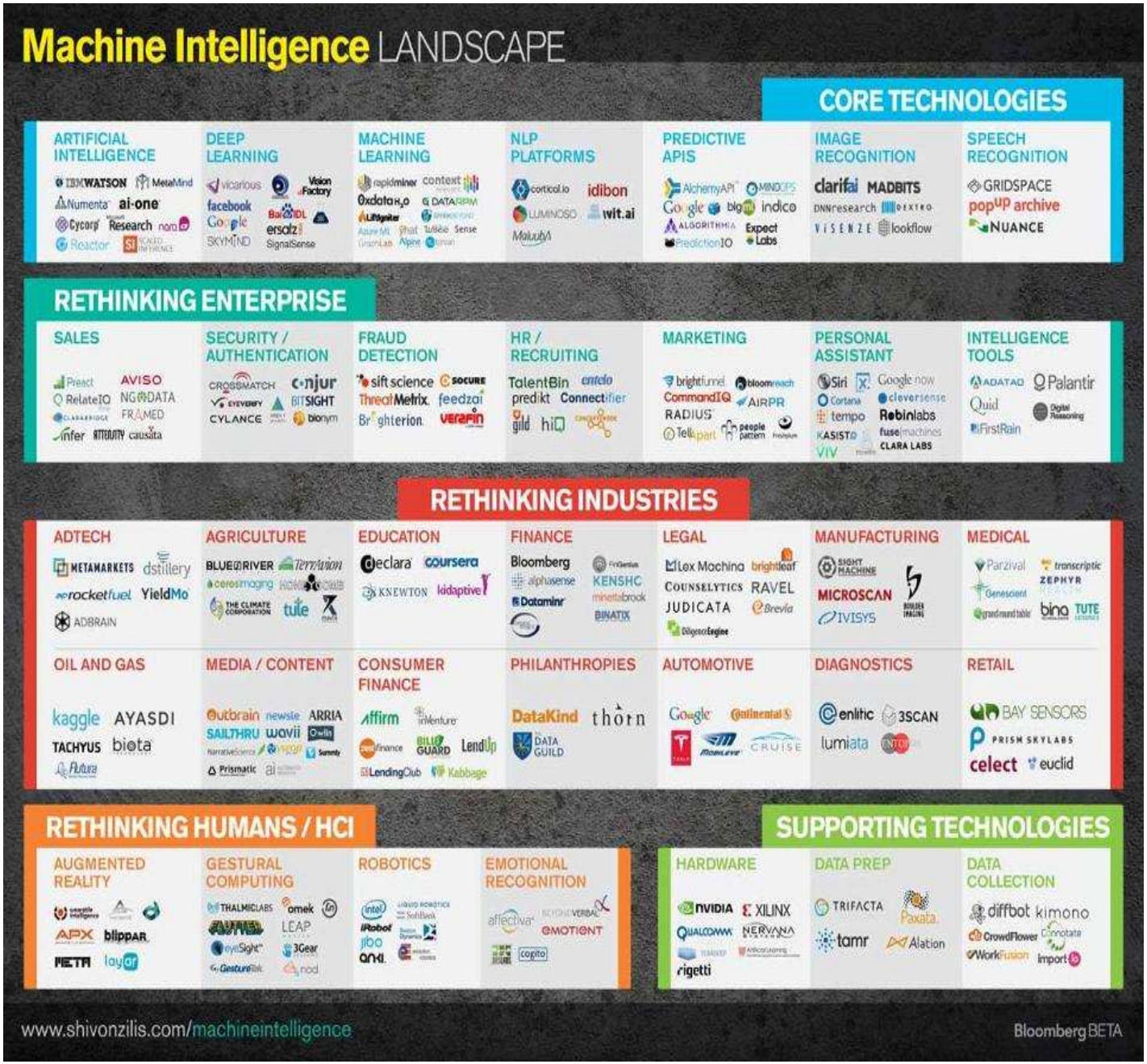
DEFINICIÓN DE BIG DATA

Volumen
Velocidad
Variedad
Veracity?

Tecnologías: ej. Inteligencia artificial (machine learning)



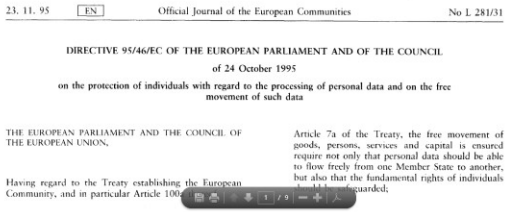
DEFINICIÓN DE BIG DATA



ALGUNOS TEXTOS DE REFERENCIA

"Your recent Amazon purchases, Tweet score and location history makes you 23.5% welcome here."

(ALGUNOS) TEXTOS DE REFERENCIA


23. 11. 95 EN Official Journal of the European Communities No L 281/31

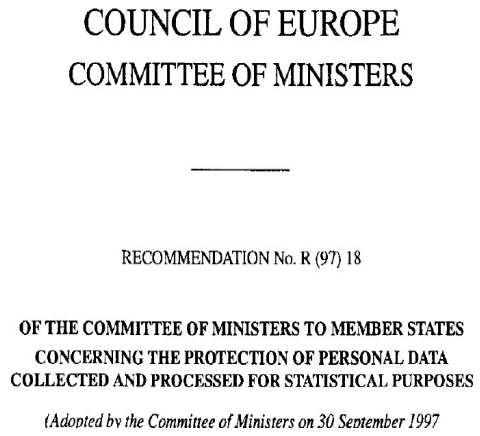
DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 24 October 1995
on the protection of individuals with regard to the processing of personal data and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a

Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals

1995

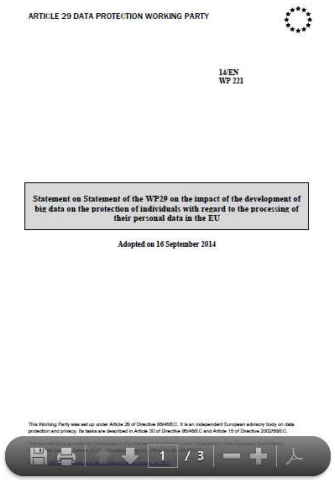

COUNCIL OF EUROPE
COMMITTEE OF MINISTERS

RECOMMENDATION No. R (97) 18

OF THE COMMITTEE OF MINISTERS TO MEMBER STATES
CONCERNING THE PROTECTION OF PERSONAL DATA
COLLECTED AND PROCESSED FOR STATISTICAL PURPOSES

(Adopted by the Committee of Ministers on 30 September 1997

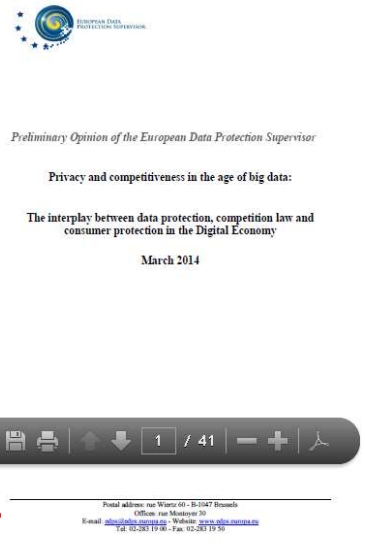
1997


ARTICLE 29 DATA PROTECTION WORKING PARTY

14/EN
WP 221

Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU

Adopted on 16 September 2014


Preliminary Opinion of the European Data Protection Supervisor

Privacy and competitiveness in the age of big data:

The interplay between data protection, competition law and consumer protection in the Digital Economy

March 2014

2014


EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 4/2015

Towards a new digital ethics

Data, dignity and technology

EDPS

11 September 2015


EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 7/2015

Meeting the challenges of big data

A call for transparency, user control, data protection by design and accountability

1 / 21

EDPS

19 November 2015

2015

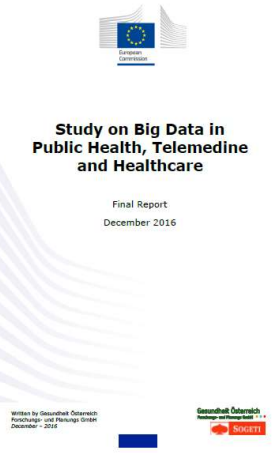

BIG DATA

A Tool for Inclusion or Exclusion?

UNDERSTANDING THE ISSUES

FTC REPORT

FEDERAL TRADE COMMISSION
JANUARY 2016


Study on Big Data in Public Health, Telemedine and Healthcare

Final Report
December 2016

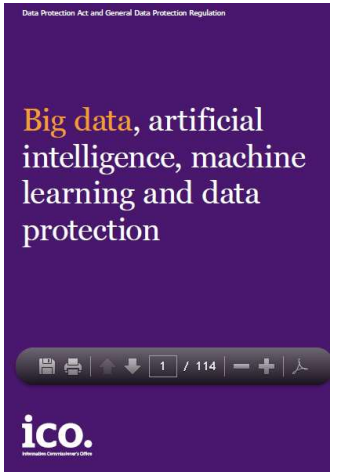

Strasbourg, 23 January 2017 T-PD(2017)01

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA
(T-PD)

GUIDELINES ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA IN A WORLD OF BIG DATA

Directorate General of Human Rights and Rule of Law

2017


Data Protection Act and General Data Protection Regulation

Big data, artificial intelligence, machine learning and data protection

1 / 114

ico.

2017

(ALGUNOS) TEXTOS DE REFERENCIA

2018

ICDPPC
International Conference of Data Protection & Privacy Commissioners

DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICAL INTELLIGENCE

40th International Conference of Data Protection and Privacy Commissioners

Tuesday 23rd October 2018, Brussels

https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

AUTHORS:

- Commission Nationale de l'Informatique et des Libertés (CNIL), France
- European Data Protection Supervisor (EDPS), European Union
- Garante per la protezione dei dati personali, Italy

CO-SPONSORS:

- Agencia de Acceso a la Información Pública, Argentina
- Commission d'accès à l'information, Québec, Canada
- Datatilsynet (Data Inspectorate), Norway
- Information Commissioner's Office (ICO), United Kingdom
- Préposé fédéral à la protection des données et à la transparence, Switzerland
- Data protection Authority, Belgium
- Privacy Commissioner for Personal Data, Hong-Kong
- Data protection Commission, Ireland
- Data Protection Office, Poland

(ALGUNOS) TEXTOS DE REFERENCIA

2018

ICDPPC
International Conference of Data Protection & Privacy Commissioners

DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICAL INTELLIGENCE

40th International Conference of Data Protection and Privacy Commissioners

Tuesday 23rd October 2018, Brussels

AUTHORS:

- Commission Nationale de l'Informatique et des Libertés (CNIL), France
- European Data Protection Supervisor (EDPS), European Union
- Garante per la protezione dei dati personali, Italy

CO-SPONSORS:

- Agencia de Acceso a la Información Pública, Argentina
- Commission d'accès à l'information, Québec, Canada
- Datatilsynet (Data Inspectorate), Norway
- Information Commissioner's Office (ICO), United Kingdom
- Préposé fédéral à la protection des données et à la transparence, Switzerland
- Data protection Authority, Belgium
- Privacy Commissioner for Personal Data, Hong-Kong
- Data protection Commission, Ireland
- Data Protection Office, Poland

CNIL.

To protect personal data, support innovation, preserve individual liberties

MY COMPLIANCE TOOLS | DATA PROTECTION | TOPICS | THE CNIL

> Algorithms and artificial intelligence: CNIL's report on the ethical issues

Algorithms and artificial intelligence: CNIL's report on the ethical issues

25 May 2018

The CNIL publishes the English version of its report on the ethical matters of algorithms and artificial intelligence, result of a public debate launched in 2017 with the help of 60 partners all over France, at a time when discussions on AI are now being carried out on the European and global stages.

The Conference therefore endorses the following guiding principles, as its core values to preserve human rights in the development of artificial intelligence:

1. Artificial intelligence and machine learning technologies should be designed, developed and used in respect of fundamental human rights and in accordance with the **fairness principle**, in particular by:

a. Considering individuals' reasonable expectations by ensuring that the use of artificial intelligence systems remains consistent with their original purposes, and that the data are used in a way that is not incompatible with the original purpose of their collection,
b. taking into consideration not only the impact that the use of artificial intelligence may have on the individual, but also the collective impact on groups and on society at large,
c. ensuring that artificial intelligence systems are developed in a way that facilitates human development and does not obstruct or endanger it, thus recognizing the need for delineation and boundaries on certain uses,

2. **Continued attention and vigilance,** as well as accountability, for the potential effects and consequences of, artificial intelligence systems should be ensured, in particular by:

a. promoting accountability of all relevant stakeholders to individuals, supervisory authorities and other third parties as appropriate, including through the realization of audit, continuous monitoring and impact assessment of artificial intelligence systems, and periodic review of oversight mechanisms;
b. fostering collective and joint responsibility, involving the whole chain of actors and stakeholders, for example with the development of collaborative standards and the sharing of best practices,
c. investing in awareness raising, education, research and training in order to ensure a good level of information on and understanding of artificial intelligence and its potential effects in society, and
d. establishing demonstrable governance processes for all relevant actors, such as relying on trusted third parties or the setting up of independent ethics committees,

3. Artificial intelligence **systems transparency and intelligibility** should be improved, with the objective of effective implementation, in particular by:

a. investing in public and private scientific research on explainable artificial intelligence,
b. promoting transparency, intelligibility and reachability, for instance through the development of innovative ways of communication, taking into account the different levels of transparency and information required for each relevant audience,
c. making organizations' practices more transparent, notably by promoting algorithmic transparency and the auditability of systems, while ensuring meaningfulness of the information provided, and
d. guaranteeing the right to informational self-determination, notably by ensuring that individuals are always informed appropriately when they are interacting directly with an artificial intelligence system or when they provide personal data to be processed by such systems,
e. providing adequate information on the purpose and effects of artificial intelligence systems in order to verify continuous alignment with expectation of individuals and to enable overall human control on such systems.

4. As part of an overall "ethics by design" approach, artificial intelligence systems should be **designed and developed responsibly**, by applying the principles of **privacy by default and privacy by design**, in particular by:

a. implementing technical and organizational measures and procedures – proportional to the type of system that is developed – to ensure that data subjects' privacy and personal data are respected, both when determining the means of the processing and at the moment of data processing,
b. assessing and documenting the expected impacts on individuals and society at the beginning of an artificial intelligence project and for relevant developments during its entire life cycle, and
c. identifying specific requirements for ethical and fair use of the systems and for respecting human rights as part of the development and operations of any artificial intelligence system,

5. **Empowerment of every individual** should be promoted, and the exercise of individuals' rights should be encouraged, as well as the creation of opportunities for public engagement, in particular by:

a. respecting data protection and privacy rights, including where applicable the right to information, the right to access, the right to object to processing and the right to erasure, and promoting those rights through education and awareness campaigns,
b. respecting related rights including freedom of expression and information, as well as non-discrimination,
c. recognizing that the right to object or appeal applies to technologies that influence personal development or opinions and guaranteeing, where applicable, individuals' right not to be subject to a decision based solely on automated processing if it significantly affects them and, where not applicable, guaranteeing individuals' right to challenge such decision,
d. using the capabilities of artificial intelligence systems to foster an equal empowerment and enhance public engagement, for example through adaptable interfaces and accessible tools.

6. Unlawful **biases or discriminations** that may result from the use of data in artificial intelligence should be reduced and mitigated, including by:

a. ensuring the respect of international legal instruments on human rights and non-discrimination,
b. investing in research into technical ways to identify, address and mitigate biases,
c. taking reasonable steps to ensure the personal data and information used in automated decision making is accurate, up-to-date and as complete as possible, and
d. elaborating specific guidance and principles in addressing biases and discrimination, and promoting individuals' and stakeholders' awareness.

Taking into consideration the principles above, the 40th International Conference of Data Protection and Privacy Commissioners calls for **common governance principles on artificial intelligence** to be established, fostering concerted international efforts in this field, in order to ensure that its development and use take place in accordance with ethics and human values, and respect human dignity. These common governance principles must be able to tackle the challenges raised by the rapid evolutions of artificial intelligence technologies, on the basis of a multi-stakeholder approach in order to address all cross-sectoral issues at stake. They must take place at an international level since the development of artificial intelligence is a trans-border phenomenon and may affect all humanity. The Conference should be involved in this international effort, working with and supporting general and sectoral authorities in other fields such as competition, market and consumer regulation.

The 40th International Conference of Data Protection and Privacy Commissioners therefore establishes, as a contribution to a future common governance at the international level, and in order to further elaborate guidance to accompany the principles on Ethics and Data Protection in Artificial Intelligence, a **permanent working group** addressing the challenges of artificial intelligence development. This **working group on Ethics and Data Protection in Artificial Intelligence** will be in charge of promoting understanding of and respect for

the principles of the present resolution, by all relevant parties involved in the development of artificial intelligence systems, including governments and public authorities, standardization bodies, artificial intelligence systems designers, providers and researchers, companies, citizens and end users of artificial intelligence systems. The working group on Ethics and Data Protection in Artificial Intelligence shall take into account the work carried out by other working groups of the Conference and shall report regularly on its activities to the Conference. The Conference thus endeavors to proactively support an active public debate on digital ethics aiming at the creation of a strong ethical culture and personal awareness in this field.

- The present declaration will be open for public consultation -

(ALGUNOS) TEXTOS DE REFERENCIA

2019 - 2020

European Commission

English

Search

Home › White Paper on Artificial Intelligence: a European approach to excellence and trust

White Paper on Artificial Intelligence: a European approach to excellence and trust

White Paper on Artificial Intelligence: a European approach to excellence and trust
19 February 2020
English (939.4 KB - PDF)

Download

Available languages (22)

AI policy observatory

OECD.AI Policy Observatory

We launched the **OECD.AI Observatory**, an online platform to shape and share AI policies across the globe, on 27 February 2020.

Watch the launch event | Agenda (English) | Ordre du jour (français) | Speaker bios

Find out more about the OECD.AI Observatory | Explore the OECD.AI Observatory

OECD Principles on Artificial Intelligence

In May 2019 the OECD adopted its **Principles on Artificial Intelligence**, the first international standards agreed by governments for the responsible stewardship of trustworthy AI.

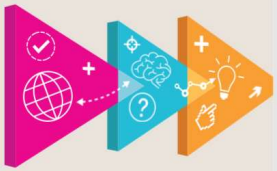
The OECD Principles on AI include concrete recommendations for public policy and strategy. The general scope of the Principles ensures they can be applied to AI developments around the world.

In our recent report **Artificial Intelligence and Society**, a chapter on **public policy considerations** reviews salient policy issues that accompany the diffusion of AI. It supports the value-based OECD Principles on AI and outlines national policies to promote trustworthy AI systems.

The **OECD.AI Policy Observatory**, launched in February 2020, aims to help policymakers implement the AI Principles.

Guidance on the AI auditing framework

Draft guidance for consultation



ico.

13 DE FEBRERO DE 2020

La AEPD publica una guía para adaptar al RGPD los productos y servicios que utilicen Inteligencia Artificial

- El documento aborda las dudas que plantea la IA en el marco de la protección de datos y recuerda los aspectos más importantes del Reglamento General de Protección de Datos que deben tenerse en cuenta desde el diseño
- Está dirigido a responsables que incorporen componentes de IA en sus tratamientos, así como a desarrolladores y encargados que den soporte a dicho tratamiento

aepd española protección datos

Adecuación al RGPD de

Dutch DPA announces three-year enforcement focus on commercial use of data and AI

November 14, 2019 - In context

The Dutch Data Protection Authority has published its supervision and enforcement priorities for 2020-2023 (in Dutch). Although the selected areas of focus are predictable, the publication gives an indication of what the enforcement risks will be for years to come. It also reveals a shift in the supervision and enforcement strategy of the data protection watchdog. Instead of setting a few annual priorities, as it has done so far, the Dutch DPA will, through 2023, target a specific set of companies with investigations stretching out over several years. The priorities indeed overlap with the strategies adopted by DPAs across Europe. After decades of relative calm, companies that process customer data for commercial purposes on a large scale should prepare for data watchdogs to knock on their door, critically questioning the commercial use or re-use of personal data. In relation to artificial intelligence, another major theme for the Dutch DPA, clients should stay ahead of the curve and prepare for the legal and ethical regulatory framework on AI that is sure to come in the near future.

The Dutch DPA announced on 11 November 2019 that through 2023, it will direct its resources towards the following three areas: commercial use or re-use of personal data (trade in data), digital government and AI & algorithms. These focus areas are generally in line with the supervision and enforcement activities of the Dutch DPA and its counterparts across Europe that we have observed in our practice.

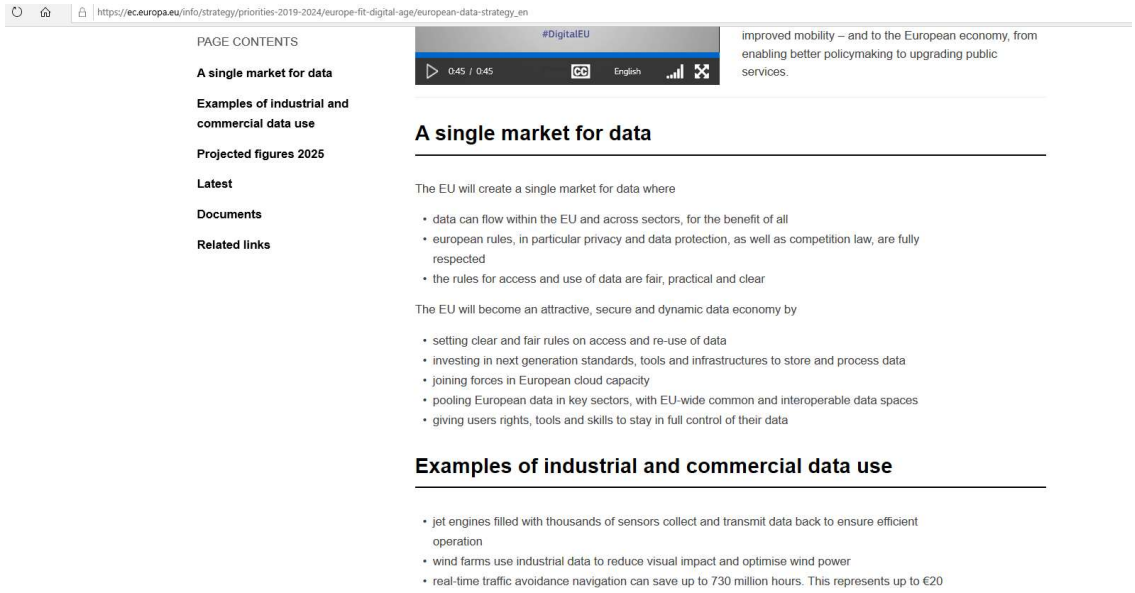
(ALGUNOS) TEXTOS DE REFERENCIA

2019 - 2020

https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

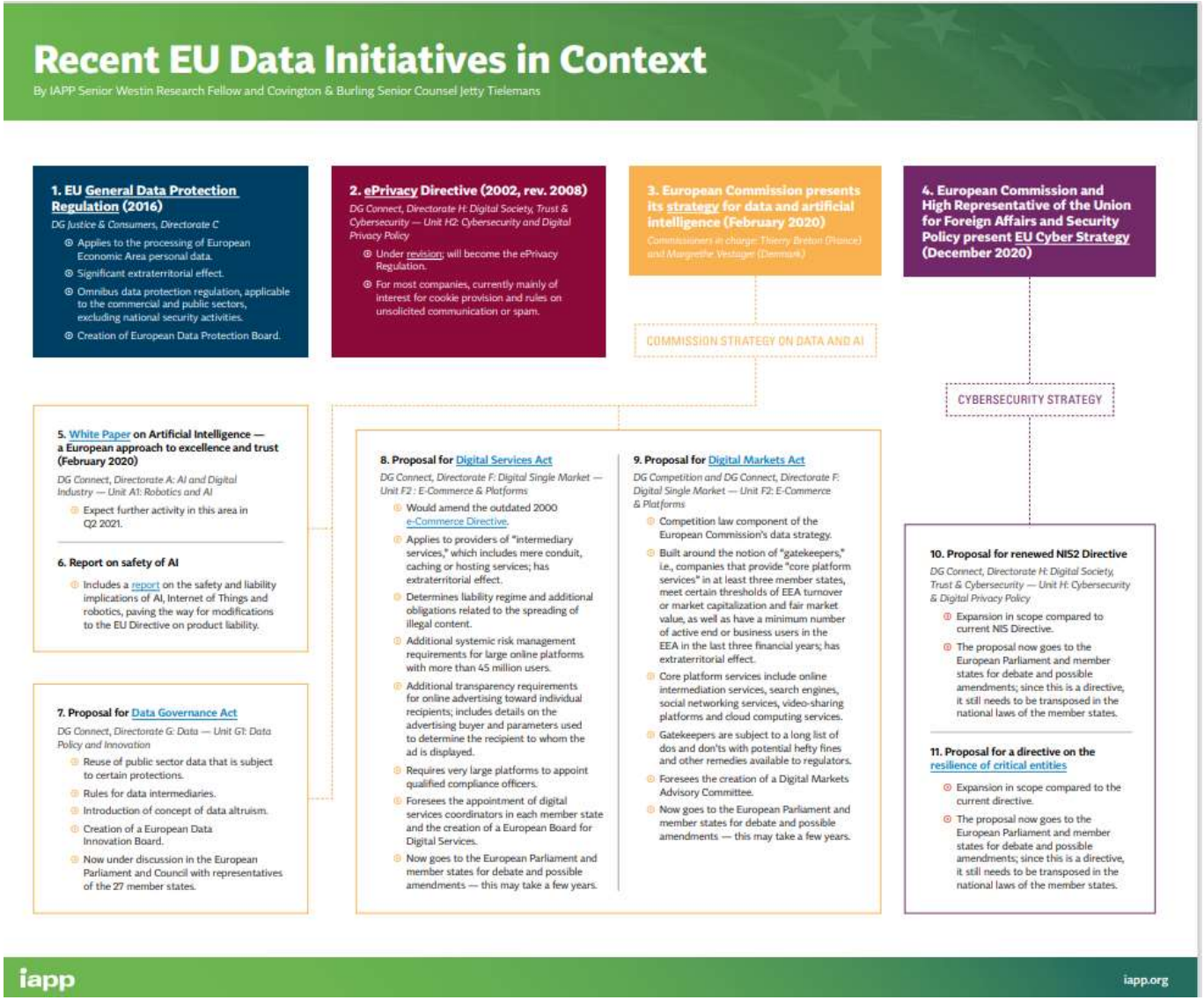
European data strategy

Making the EU a role model for a society empowered by data.



(ALGUNOS) TEXTOS DE REFERENCIA

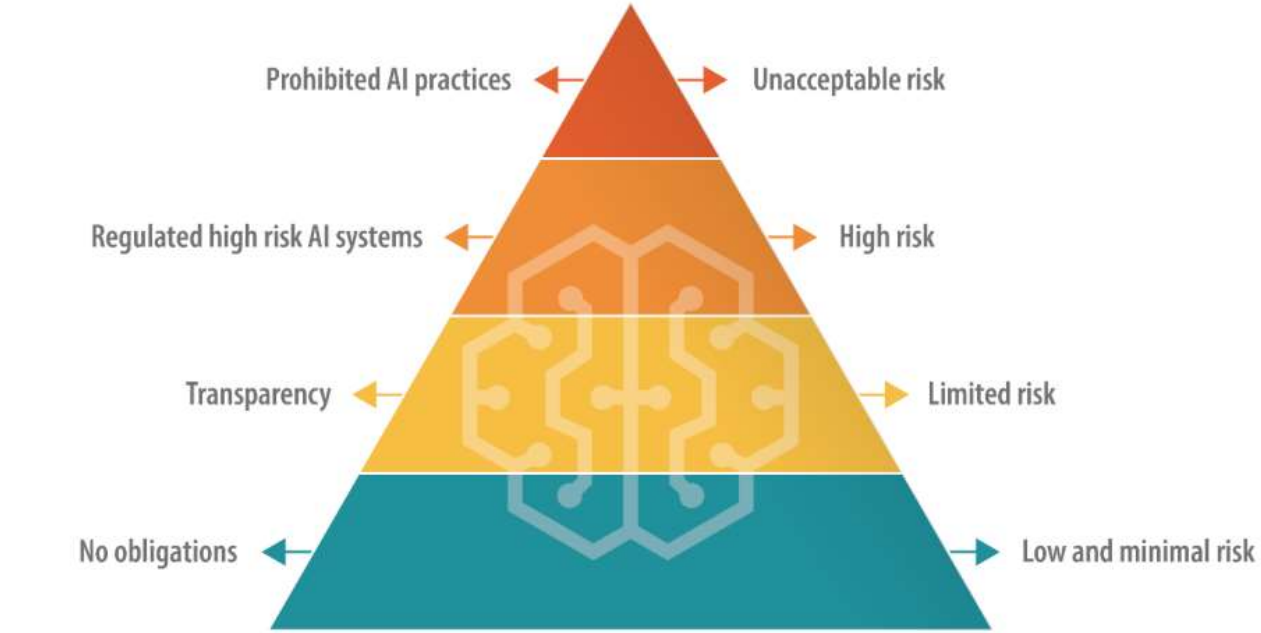
2021



(ALGUNOS) TEXTOS DE REFERENCIA

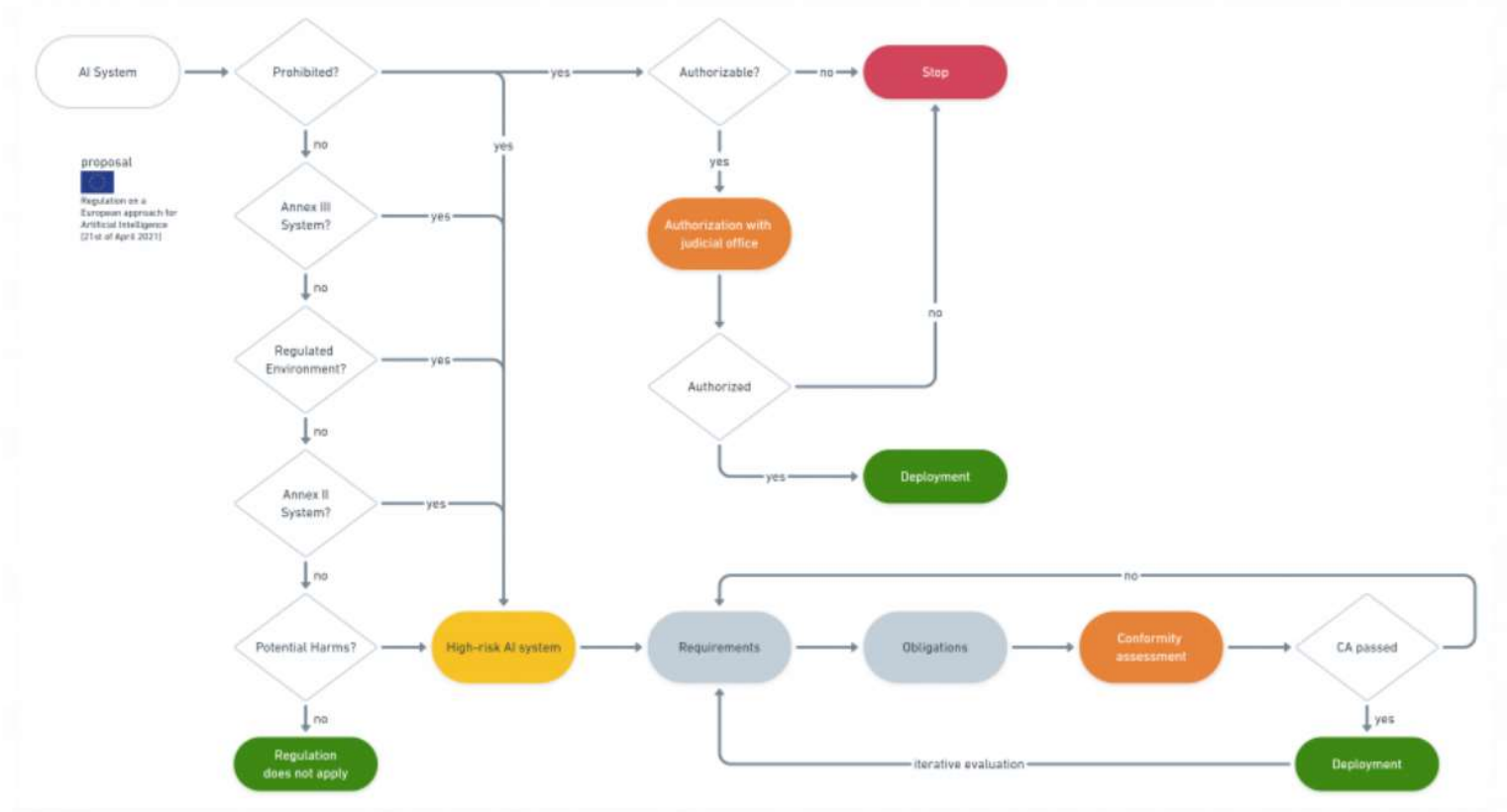
Unacceptable-risk AI systems	High-risk AI systems	Limited- and minimal-risk AI systems
• Subliminal, manipulative, or exploitative techniques causing harm • Real-time, remote biometric identification systems used in public spaces for law enforcement • All forms of social scoring	• Systems that evaluate consumer creditworthiness • Recruiting or employee-management systems • Systems utilizing biometric identification in nonpublic spaces • Safety-critical systems (eg, systems that would put the health of citizens at risk due to failure) • Any systems used in the administration of justice	• AI chatbots • AI-enabled video and computer games • Spam filters • Inventory-management systems • Customer- and market-segmentation systems • Most other AI systems

(ALGUNOS) TEXTOS DE REFERENCIA



Data source: European Commission.

(ALGUNOS) TEXTOS DE REFERENCIA



(ALGUNOS) TEXTOS DE REFERENCIA

31995L0046

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Official Journal L 281 , 23/11/1995 P. 0031 - 0050

Article 15

Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

Article 22

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

(ALGUNOS) TEXTOS DE REFERENCIA

COUNCIL OF EUROPE

COMMITTEE OF MINISTERS

RECOMMENDATION No. R (97) 18

OF THE COMMITTEE OF MINISTERS TO MEMBER STATES
CONCERNING THE PROTECTION OF PERSONAL DATA
COLLECTED AND PROCESSED FOR STATISTICAL PURPOSES

(Adopted by the Committee of Ministers on 30 September 1997

4. General conditions for lawful collection and processing for statistical purposes

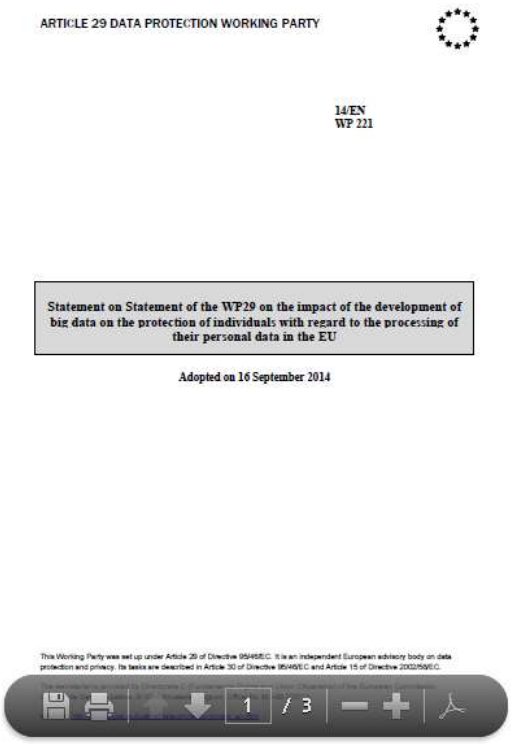
Purpose

4.1. Personal data collected and processed for statistical purposes shall serve only those purposes. They shall not be used to take a decision or measure in respect of the data subject, nor to supplement or correct files containing personal data which are processed for non-statistical purposes.

4.2. Processing for statistical purposes of personal data collected for non-statistical purposes is not incompatible with the purpose(s) for which the data were initially collected if appropriate safeguards are provided for, in particular to prevent the use of data for supporting decisions or measures in respect of the data subject.

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680508d7e

(ALGUNOS) TEXTOS DE REFERENCIA



ARTICLE 29 DATA PROTECTION WORKING PARTY

14/EN
WP 221

Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU

Adopted on 16 September 2014

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

1 / 3

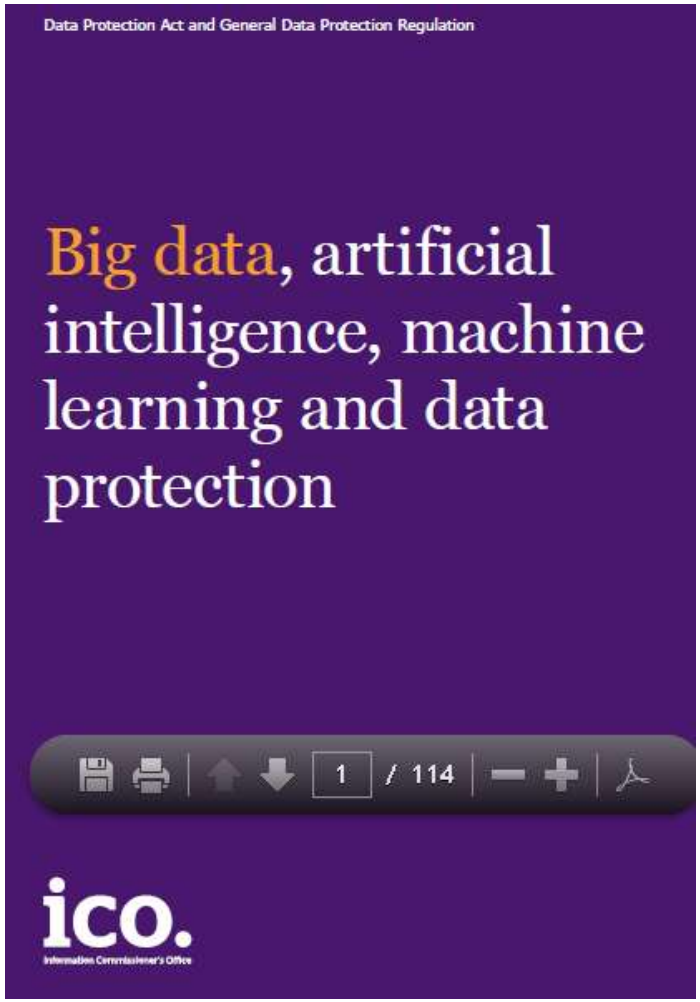
- "Big data" is a broad term that covers a great number of data processing operations, some of which are already well-identified, while others are still unclear and many more are expected to be developed in the near future.

- In addition, big data processing operations do not always involve personal data. Nevertheless, the retention and analysis of huge amounts of personal data in big data environments require particular attention and care. Patterns relating to specific individuals may be identified, also by means of the increased availability of computer processing power and data mining capabilities.

- A number of developments that are qualified today as big data – such as the development of comprehensive information systems in the delivery of health services or in the centralisation of law enforcement files, as well as behavioural advertising – have long been implemented in many EU Member States. These have already been addressed within the framework of the existing data protection rules, whether at EU or national levels.

- On the basis of these shared experiences, the Working Party recently released a number of policy documents which are relevant to the analysis of privacy concerns raised with regard to big data – e.g. Opinion 03/2013 on Purpose limitation, Opinion 05/2014 on Anonymisation techniques, Opinion 6/2014 on Legitimate interests or Opinion 01/2014 on the Application of necessity and proportionality concepts and data protection within the law enforcement sector.

ASPECTOS DISTINTIVOS

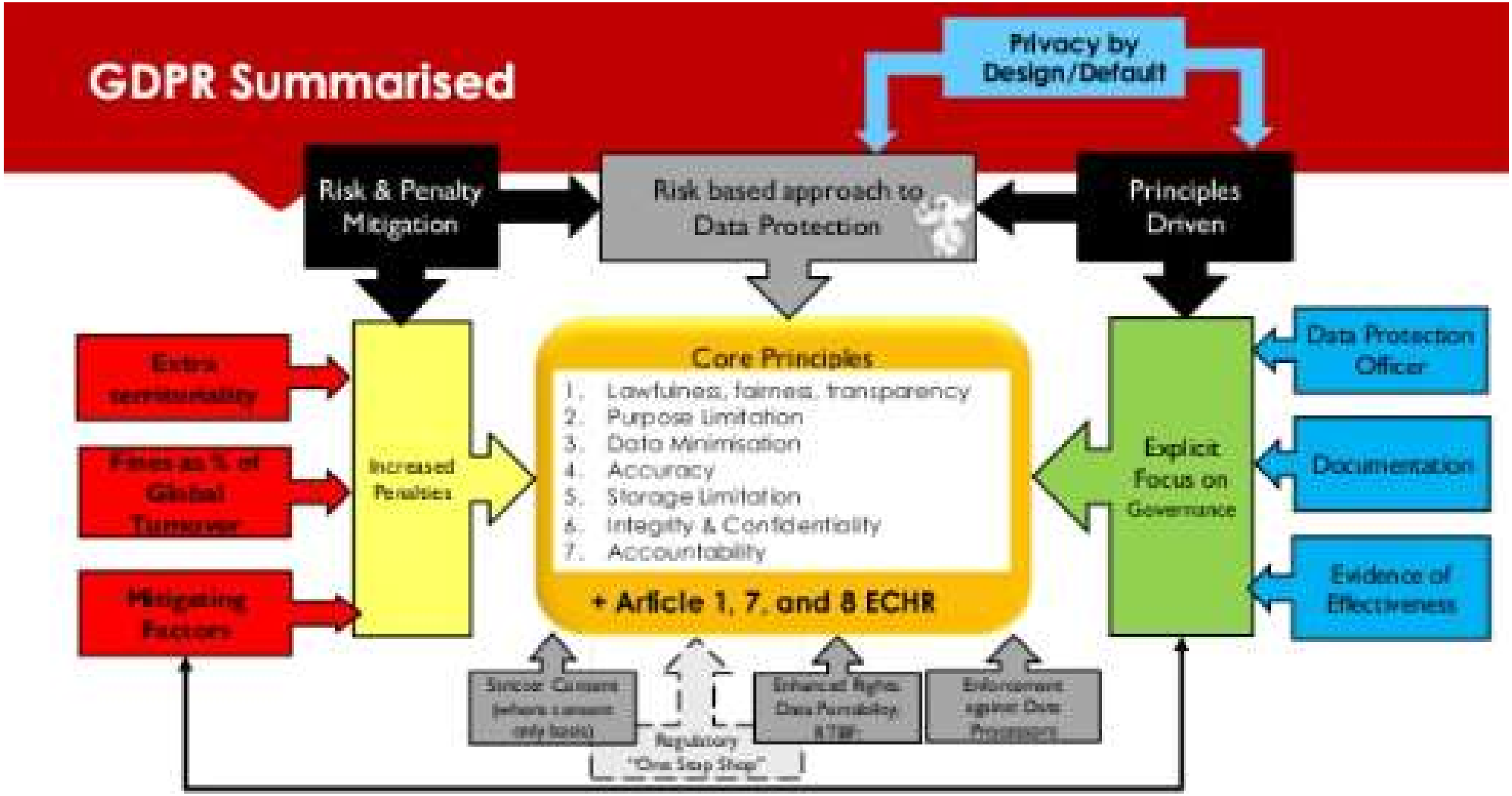


Some of the distinctive aspects of big data analytics are:

- the use of algorithms
- the opacity of the processing
- the tendency to collect 'all the data'
- the repurposing of data, and
- the use of new types of data.

  - **Provided data** is consciously given by individuals, eg when filling in an online form.
  - **Observed data** is recorded automatically, eg by online cookies or sensors or CCTV linked to facial recognition.
  - **Derived data** is produced from other data in a relatively simple and straightforward fashion, eg calculating customer profitability from the number of visits to a store and items bought.
  - **Inferred data** is produced by using a more complex method of analytics to find correlations between datasets and using these to categorise or profile people, eg calculating credit scores or predicting future health outcomes. Inferred data is based on probabilities and can thus be said to be less 'certain' than derived data.

(ALGUNOS) TEXTOS DE REFERENCIA



(ALGUNOS) TEXTOS DE REFERENCIA

Brussels, 10.1.2017
COM(2017) 10 final

2017/0003 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

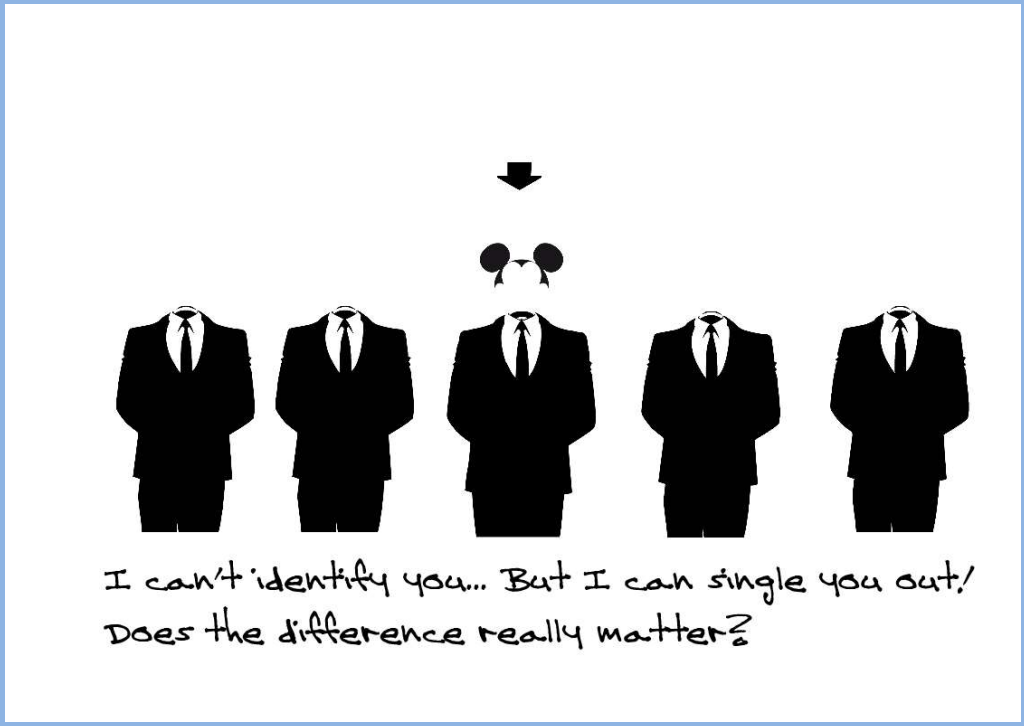
(Text with EEA relevance)

{SWD(2017) 3 final}
{SWD(2017) 4 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

The proposal for a regulation on high level of privacy rules for all electronic communications includes:

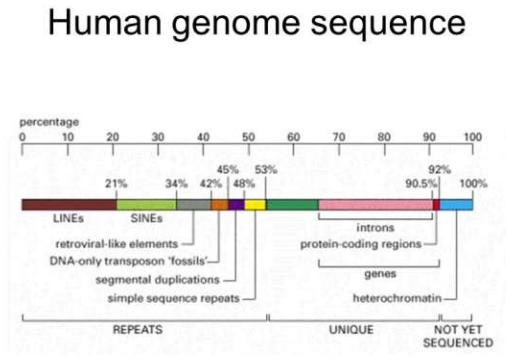
- **New players**: privacy rules will in the future also apply to new players providing electronic communications services such as WhatsApp, Facebook Messenger and Skype. This will ensure that these popular services guarantee the same level of confidentiality of communications as traditional telecoms operators.
- **Stronger rules**: all people and businesses in the EU will enjoy the same level of protection of their electronic communications through this directly applicable regulation. Businesses will also benefit from one single set of rules across the EU.
- **Communications content and metadata**: privacy is guaranteed for communications content and metadata, e.g. time of a call and location. Metadata have a high privacy component and is to be anonymised or deleted if users did not give their consent, unless the data is needed for billing.
- **New business opportunities**: once consent is given for communications data - content and/or metadata - to be processed, traditional telecoms operators will have more opportunities to provide additional services and to develop their businesses. For example, they could produce heat maps indicating the presence of individuals; these could help public authorities and transport companies when developing new infrastructure projects.
- **Simpler rules on cookies**: the cookie provision, which has resulted in an overload of consent requests for internet users, will be streamlined. The new rule will be more user-friendly as browser settings will provide for an easy way to accept or refuse tracking cookies and other identifiers. The proposal also clarifies that no consent is needed for non-privacy intrusive cookies improving internet experience (e.g. to remember shopping cart history) or cookies used by a website to count the number of visitors.
- **Protection against spam**: this proposal bans unsolicited electronic communications by emails, SMS and automated calling machines. Depending on national law people will either be protected by default or be able to use a do-not-call list to not receive marketing phone calls. Marketing callers will need to display their phone number or use a special pre-fix that indicates a marketing call.
- **More effective enforcement**: the enforcement of the confidentiality rules in the Regulation will be the responsibility of data protection authorities, already in charge of the rules under the General Data Protection Regulation.

PRINCIPIOS BÁSICOS DE PROTECCIÓN DE DATOS PERSONALES



PRINCIPIOS BÁSICOS

¿Qué es dato personal?



'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, ***in particular by reference to an identifier*** *such as a name, an identification number,* ***location data, an online identifier*** *or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;* [GDPR]

PRINCIPIOS BÁSICOS

¿Qué es dato personal?

De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

https://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_constitucional/common/pdfs/Sentencia292.pdf

PRINCIPIOS BÁSICOS

¿Qué es dato personal?

As regards "indirectly" identified or identifiable persons, this category typically relates to the phenomenon of "unique combinations", whether small or large in size. In cases where *prima facie* the extent of the identifiers available does not allow anyone to single out a particular person, that person might still be "identifiable" because that information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from others . This is where the Directive comes in with "one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". Some characteristics are so unique that someone can be identified with no effort ("present Prime Minister of Spain"), but a combination of details on categorical level (age category, regional origin, etc) may also be pretty conclusive in some circumstances, particularly if one has access to additional information of some sort. This phenomenon has been studied extensively by statisticians, always keen to avoid a breach of confidentiality.

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

PRINCIPIOS BÁSICOS

¿Qué es dato personal?

Info. que, por sí misma o en combinación con otra fácilmente disponible, nadie pueda identificar o relacionar con un individuo vivo

Figure 32 contains a summary of the results reported in the previous section. A description of each reported percentage is provided in the following paragraphs. These percentages demonstrate how combinations of characteristics can combine to narrow the number of possible people under consideration as the subject of de-identified person-specific data.

County	18.1	0.04	0.00004	0.00000*
Place	58.4	3.6	0.04	0.01
ZIP	87.1	3.7	0.04	0.01
	DOB	**Mon/Year**	**BirthYear**	**2yr Age**

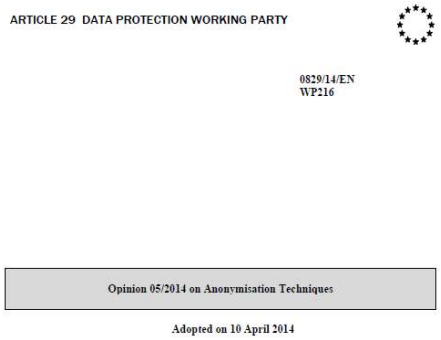
Figure 32 Percentage of US population identified with gender as geography and age vary

Experiment B reported that 87.1% (216 million of 248 million) of the population in the United States had characteristics that were likely made them unique based only on {*5-digit ZIP*, *gender*, *date of birth*}. Experiment C reported that 3.7% of the population in the United States had characteristics that were likely made them unique based only on {*5-digit ZIP*, *gender*, *Month and year of birth*}. Experiment D reported that 0.04% of the population in the United States had characteristics that were likely made them unique based only on {*5-digit ZIP*, *gender*, Year *of birth*}. Experiment E reported that 0.01% of the population in the United States had

http://dataprivacylab.org/projects/identifiability/paper1.pdf

PRINCIPIOS BÁSICOS

¿Qué es dato personal?


ARTICLE 29 DATA PROTECTION WORKING PARTY

0829/14/EN
WP216

Opinion 05/2014 on Anonymisation Techniques

Adopted on 10 April 2014

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

- Article 29 Opinion on anonymisation provides **two options** to establish if a dataset is anonymised:

1. Demonstrate that after anonymisation it is no longer possible to:
   - *Singling out:* possibility to isolate some records of an individual in the dataset*;
   - *Linkability:* ability to link, at least, two records concerning the same data subject or a group of data subjects (in the same database or in two different databases);
   - *Inference:* the possibility to deduce, with significant probability, the value of an attribute from the values of a set of other attributes

OR

2. Perform an analysis of re-identification risk.

* In the context of phase 1 of policy 0070, dataset are the set of clinical reports published by the Agency

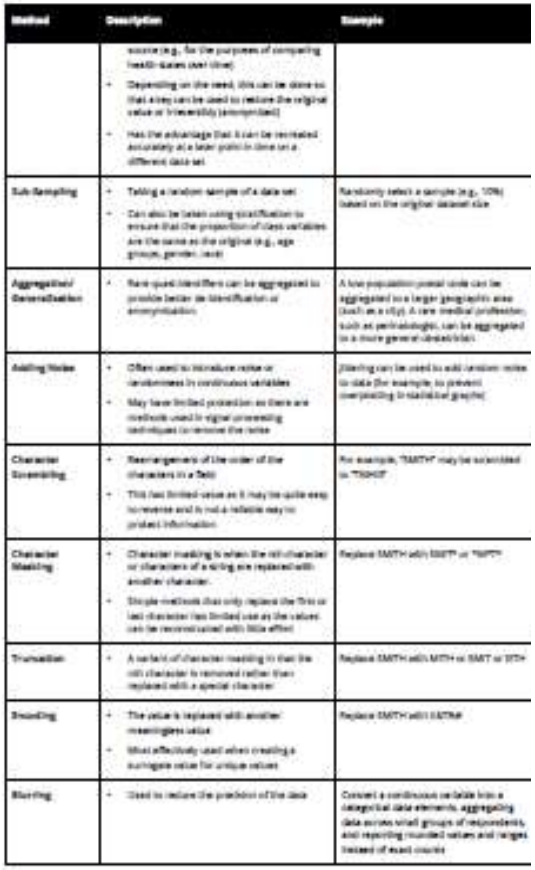
http://www.ema.europa.eu/docs/en_GB/document_library/Presentation/2015/06/WC500188859.pdf

PRINCIPIOS BÁSICOS

¿Qué es dato personal?

As stated above, de-identification refers to the removal of fields as stored in systems as we minimize the risk that identifiable information can be used to reconstruct an individual's record. De-identification methods include:

Method	Description	Example
Record Suppression	• Removing data (e.g., from a cell or a row) to prevent the identification of individuals in small groups or those with unique characteristics • When the combination of quasi-identifiers (e.g., sex, race, zip code, diagnosis) presents too high a risk of re-identification to be released • Often used in public health reporting, geo-spatial analytics or secondary use datasets • This method may result in the loss of fidelity for small subgroups • Usually requires additional suppression of non-sensitive data to ensure adequate protection of PII (e.g., complementary suppression of one or more non-sensitive cells in a table so that the values of the suppressed cells may not be calculated by subtracting the reported values from the row and column totals)	Drop the observations for those patients where the number of patients for any combination of zip code, age category and diagnosis code is below a given threshold (e.g., 5 people)
Cell Suppression	• Suppressing or masking the value of a single field	A field in a patient record containing a very rare disease
Randomization	• Retains the direct identifiers (name, phone number), but replaces their values with simulated (random) values • Reduces the probability of reverse identification • Often used in creating data sets for software testing where all fields must be present and have realistic looking values	Algorithm which randomly replaces the date of birth for patients
Shuffling	• Data for one or more variables are switched with another record • Often used in creating data sets for software testing where all fields must be present and have realistic looking values • All of the values in the data set are real, but they are assigned to the wrong people	Distinct values of a variable are randomly assigned to records
Creating Pseudonyms or Surrogate	• The creation of aliases can be done in one of two ways where a variable such as SSN or medical record number is replaced with a surrogate • Refers to the unique descriptor that can be used to match individual level records across de-identified data files from the same source (e.g., for the purposes of comparing health-states over time) • Depending on the need, this can be done so that a key can be used to restore the original value or irreversibly (anonymized) • Has the advantage that it can be recreated accurately at a later point in time on a different data set	Applying a one-way hash to the variable using a secret (protected) key. A hash is a function that converts a value to another value (the hash value) but you cannot reverse the hash value back to the original value



Method	Description	Example
Sub-Sampling	• Taking a random sample of a data set • Can also be taken using stratification to ensure that the proportion of class variables are the same as the original (e.g., age groups, gender, race)	Randomly select a sample (e.g., 10%) based on the original dataset size
Aggregation/ Generalization	• Rare quasi-identifiers can be aggregated to provide better de-identification or anonymization	A low population postal code can be aggregated to a larger geographic area (such as a city). A rare medical profession, such as perinatologist, can be aggregated to a more general classification
Adding Noise	• Often used to introduce noise or randomness in continuous variables • May have limited protection as there are methods used in signal processing techniques to remove the noise	Jittering can be used to add random noise to data (for example, to prevent overplotting in statistical graphs)
Character Scrambling	• Rearrangement of the order of the characters in a field • This has limited value as it may be quite easy to reverse and is not a reliable way to protect information	For example, "SMITH" may be scrambled to "HSMIT"
Character Masking	• Character masking is when the nth character or characters of a string are replaced with another character • Simple methods that only replace the first or last character has limited use as the values can be reconstructed with little effort	Replace SMITH with SMITH or "SMTT"
Truncation	• A variant of character masking in that the nth character is removed rather than replaced with a special character	Replace SMITH with MITH or SMIT or ITH
Binning	• The value is replaced with another meaningless value • Most effectively used when creating a surrogate value for unique values	Replace SMITH with EATNH
Blurring	• Used to reduce the precision of the data	Convert a continuous variable into a categorical data elements, aggregating data across small groups of respondents, and reporting rounded values and ranges instead of exact counts

Method	Description	Example
		Replace an individual's actual reported value with the average group value (or more than one variable with different groupings for each variable)
Masking	• Used to "mask" the original values in a data set • The purpose of this technique is to retain the structure and functional usability of the data while concealing information that could lead to the identification, either directly or indirectly, of an individual value	Replace sensitive information with realistic but fake data Modify original data values based on pre-determined masking rules (e.g., by applying a transformation algorithm)
Perturbation	• Involves making small changes to the data to prevent identification of individuals from unique or rare population groups • Data perturbation is a data masking technique in that it is used to "mask" the original values in a data set to avoid disclosure	Swap data among individual cells to introduce uncertainty, so that the consumer of the data does not know whether the real data values correspond to certain records, and introduce "noise" or errors (e.g., by randomly misclassifying values of a categorical variable)
Redaction	• The process of expunging sensitive data from the records prior to disclosure	All identifiers and quasi-identifiers are dropped from the dataset

Table 1: Types of De-identification Methods

It is important to keep in mind that even the masking techniques that are protective will significantly reduce the utility of the data. Therefore, masking should be applied only to the fields that will not be used in any data analysis, which are often the direct identifiers fields such as names and email addresses that are not usually part of any analysis performed on the data. Also, one should not apply masking techniques to dates or geographic information because these fields are often used in data analysis, and masking would make it very difficult to perform an analysis using those fields.

De-identification is based on characteristics of the different variables and field type. For instance, different algorithms are applied to dates of birth than zip codes. A detailed discussion of the de-identification algorithms that we use can be found here - (K. El Emam et al., 2009). Because many data sets consist of both quasi-identifiers and direct identifiers, in practice it is important to apply both data protection techniques: masking and de-identification.

Data Protection Maturity

Techniques for Ensuring Data Privacy for Analytics

As analytics professionals it is our duty to ensure that the data that we access, integrate, analyze and disseminate carry the expectation of privacy access is controlled proactively. In our consulting practice, we often see data protection measures focus on the protection of data in source systems and in

15

PRINCIPIOS BÁSICOS

¿Qué es dato personal?

Riesgo de re-identificación razonable

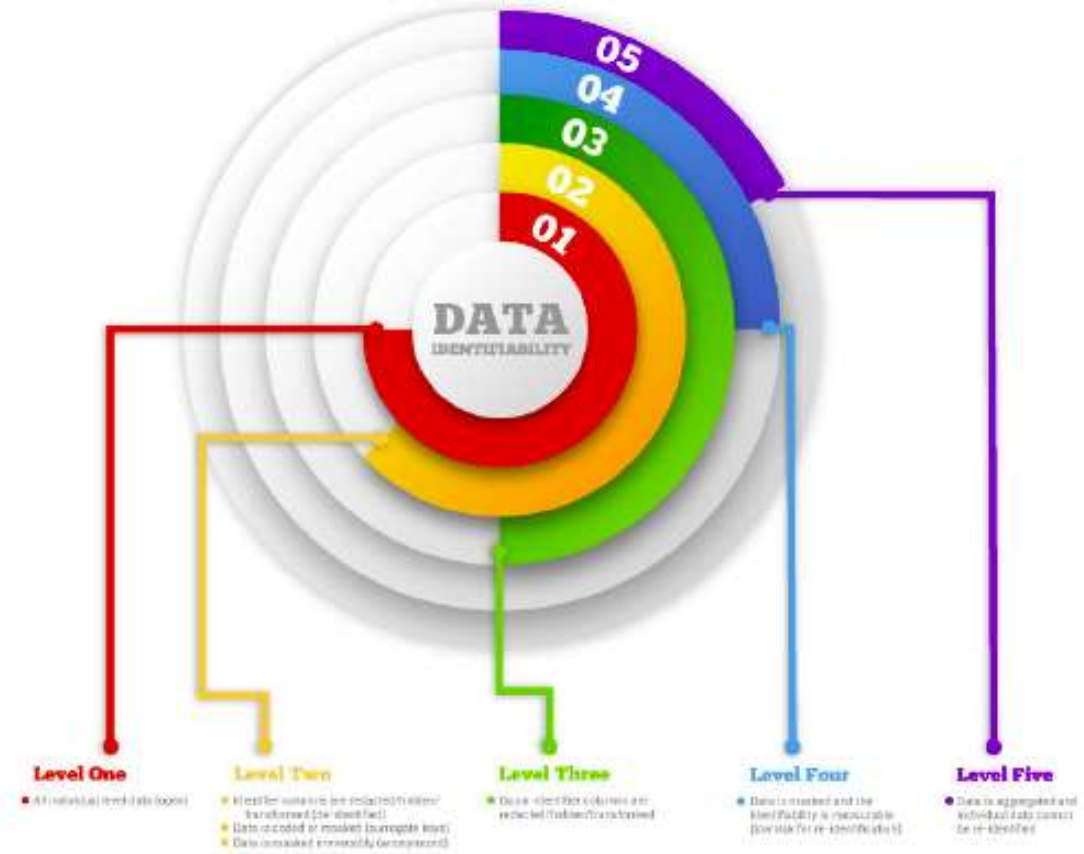


Figure 6: Data Identifiability Continuum.

PRINCIPIOS BÁSICOS

Información

- ¿Quién/es?
- ¿Para qué? **Finalidad específica**
- [¿Dónde?]: UE/ no UE + salvaguardas
- [Ejercicio de derechos] ARCO y derechos nuevos (portabilidad, olvido…)
- Plazos de retención

*** GDPR**

PRINCIPIOS BÁSICOS

Información

Política de protección de datos = ¿texto estándar?

Política de Protección de Datos

Los datos personales que nos aporte serán objeto de tratamiento en un fichero con las finalidades de, entre otros supuestos que se podrán especificar en cada caso, atender las solicitudes que nos plantee, remitirle la información solicitada, así como en su caso, gestionar su acceso a determinados servicios o funcionalidades del Sitio Web, por parte de Industria de Diseño Textil S.A., con domicilio social en Avda. de la Diputación, Edificio Inditex, 15142, Arteixo, A Coruña (España), como responsable del fichero. Inditex, S.A. se compromete a respetar la confidencialidad de la información de carácter personal y a garantizar el ejercicio de tus derechos de acceso, rectificación, cancelación y oposición, que podrás ejercitar mediante comunicación escrita dirigida a dirección anteriormente indicada a la atención de "Función LOPD", o mediante el envío de un correo electrónico a funcionlopd@inditex.com. En caso necesario, para atender su solicitud podremos requerir la aportación de una fotocopia de su DNI, pasaporte u otro documento válido que lo identifique.

Para cumplir con las mencionadas finalidades, puede resultar necesario que comuniquemos la información que nos ha proporcionado a determinadas sociedades integrantes del Grupo Inditex (cuyas actividades se relacionan con los sectores de e-commerce, decoración, textil, de productos acabados de vestir y del hogar, así como con cualesquiera otros complementarios de los anteriores, incluidos los de cosmética y marroquinería) por lo que entendemos que, al registrarse y/o proporcionarnos información a través de este Sitio Web o a través de otros medios como el correo electrónico, nos autoriza expresamente para efectuar tales comunicaciones a dichas sociedades pertenecientes al Grupo Inditex.

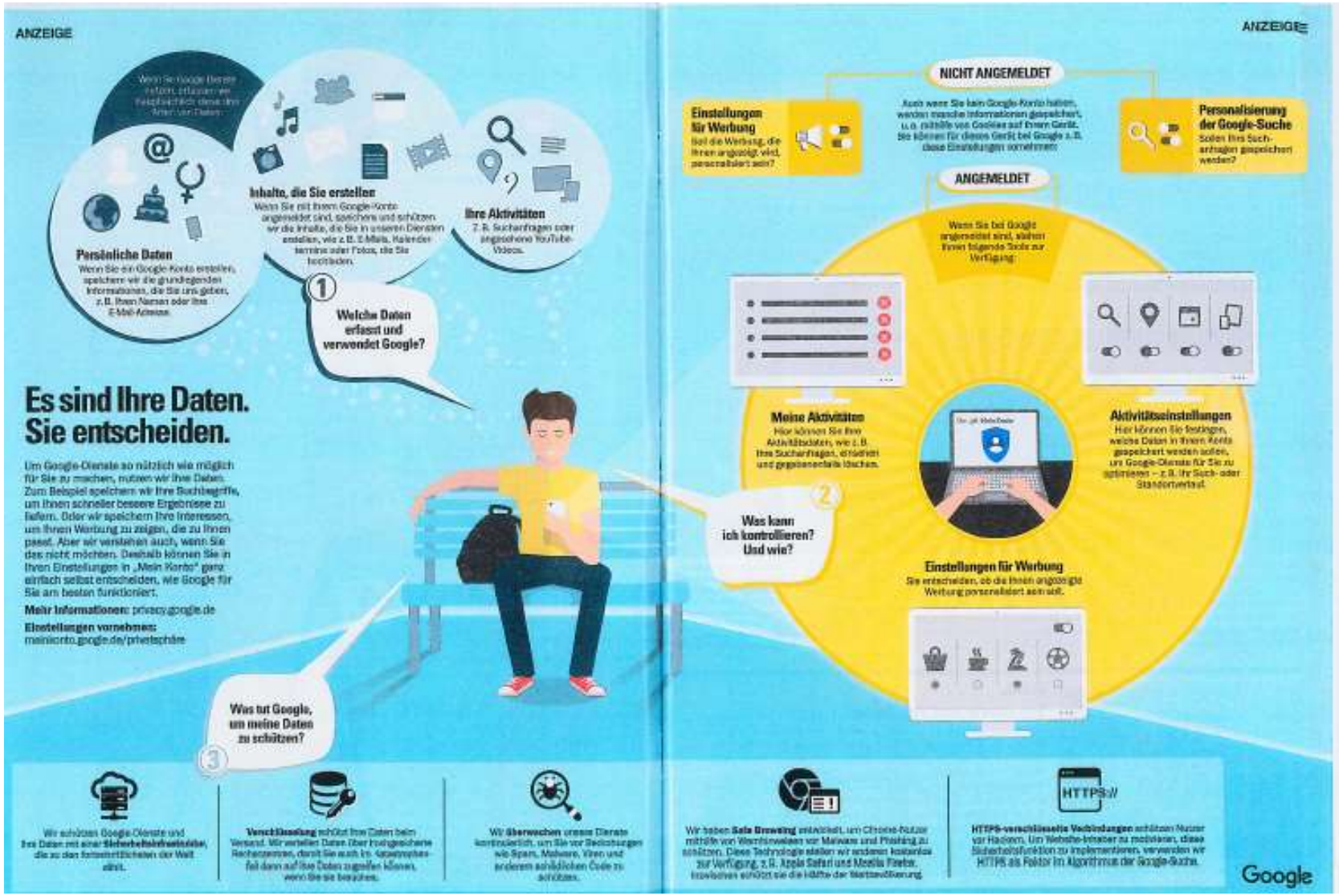
Información sobre Cookies: En este Sitio Web utilizamos cookies, pequeños ficheros de texto con información sobre su navegación en este sitio, cuyo principal objetivo es mejorar su experiencia en la web. Puede encontrar más información sobre las cookies que utilizamos, su finalidad y otra información de interés en el siguiente enlace: http://www.inditex.com/es/cookies.

Aceptando la presente política de privacidad consiente la utilización de las cookies utilizadas en este Sitio Web y que se describen en la página anteriormente indicada.

PRINCIPIOS BÁSICOS

Información

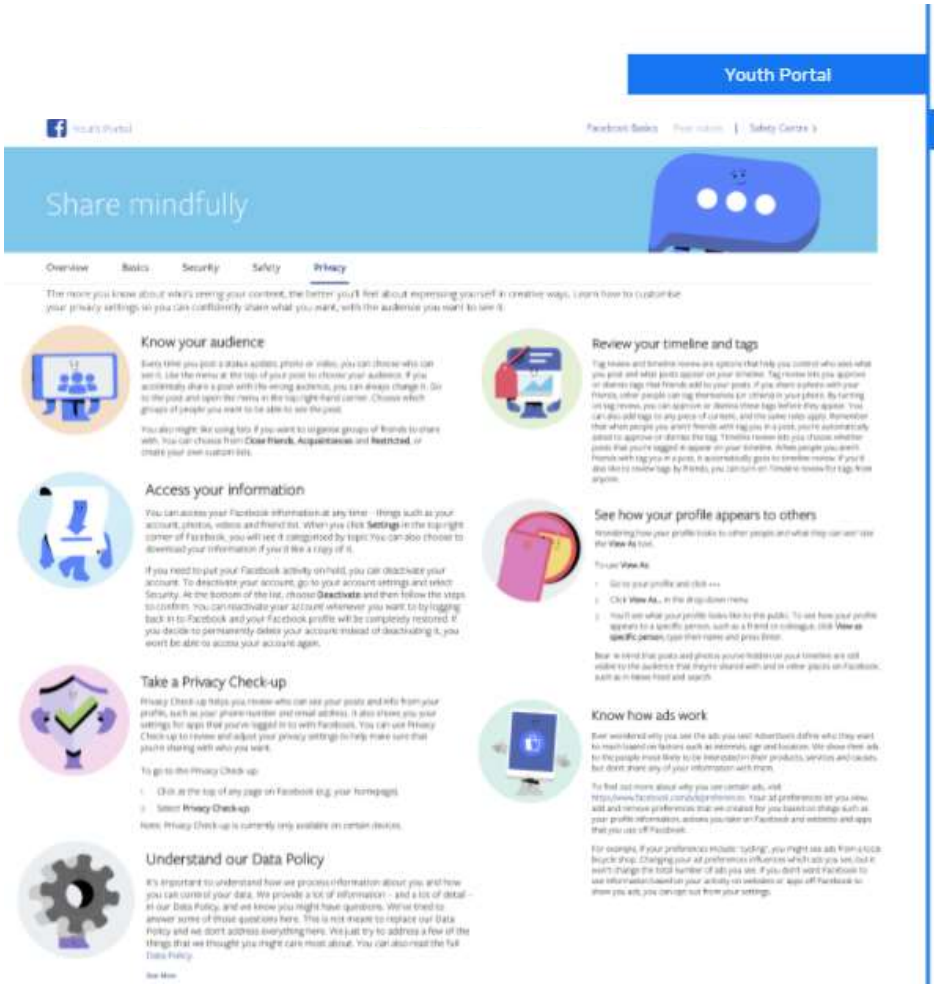
Política de protección de datos = ¿un texto?

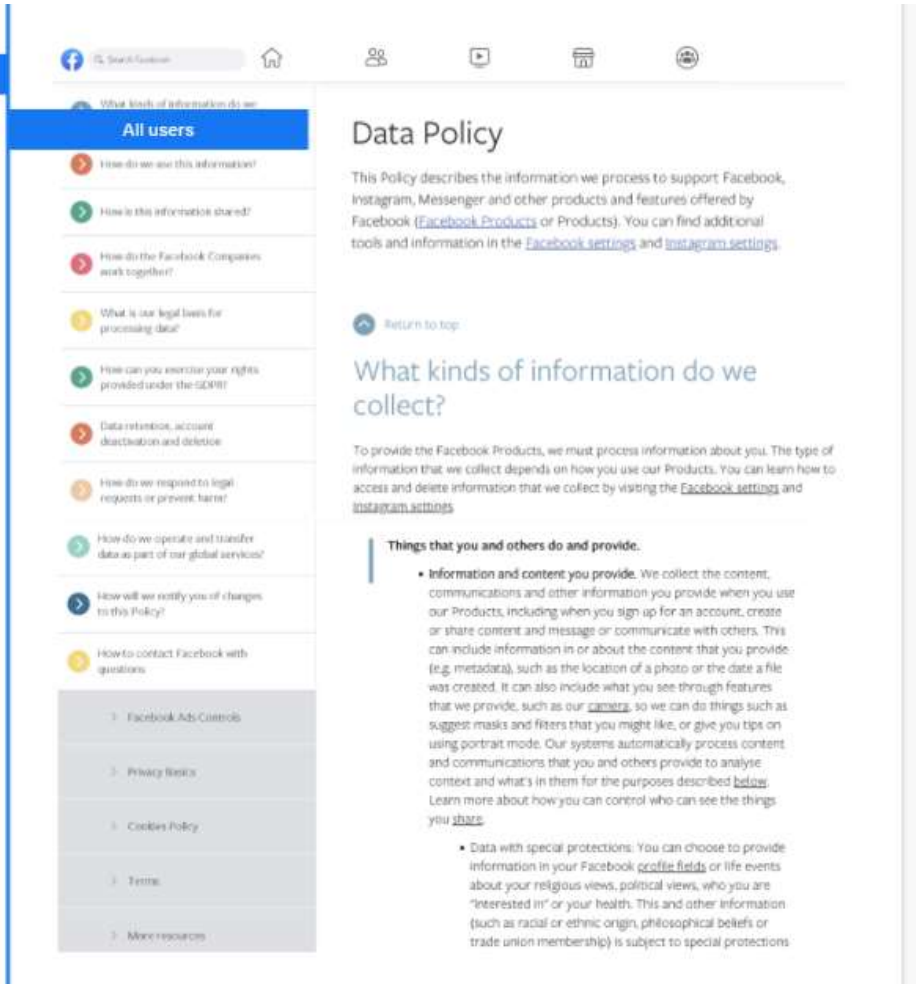


PRINCIPIOS BÁSICOS

Información

Política de protección de datos = ¿diferentes audiencias, diferente presentación?





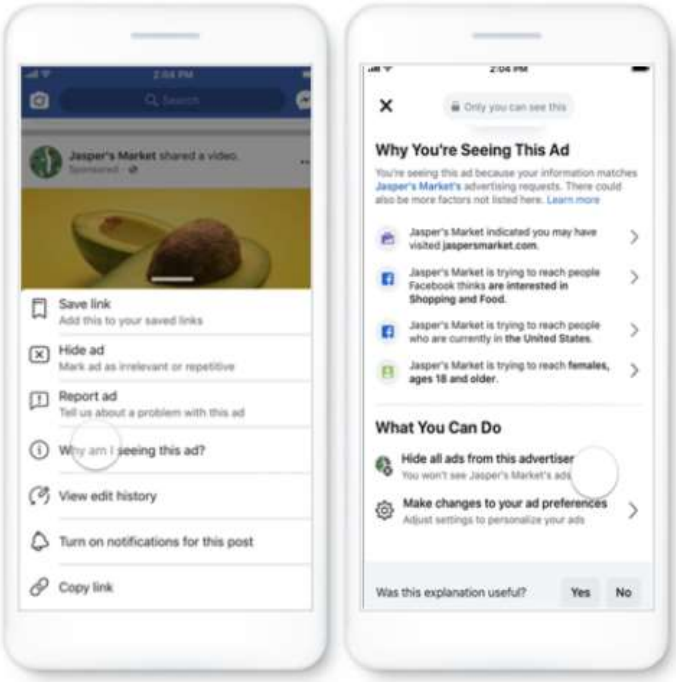
PRINCIPIOS BÁSICOS

Información

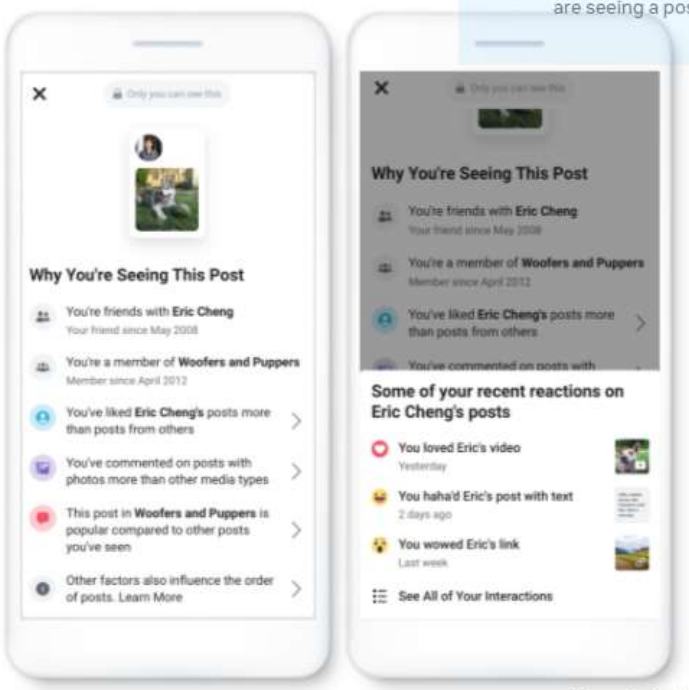
Transparencia algorítmica

WAIST
(Why Am I Seeing This?)

Show users different reasons why they are seeing a post and an ad



Why Am I Seeing This Ad?



Why Am I Seeing This Post?

*Examples for illustrative purpose

PRINCIPIOS BÁSICOS

Consentimiento / otras causas de legitimación

Dº a la protección de datos

=

Dº a decidir <u>con quién</u> y <u>para qué</u> se utilizan <u>mis</u> datos

*"'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, **by a statement or by a clear affirmative action**, signifies agreement to the processing of personal data relating to him or her"*

PRINCIPIOS BÁSICOS

Consentimiento / Otras causas de legitimación / Usos compatibles

¿Otros bienes jurídicos prevalentes?

- Contrato
- Ley (EU/Estado miembro)
- Interés público importante
- Interés legítimo: balance de intereses (N/A en caso de **datos sensibles*** o sector público)

Salud, vida sexual, opiniones políticas, pertenencia a sindicatos, creencias religiosas, comisión de infracciones penales o administrativas

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

   (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

   (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

   (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

   (d) the possible consequences of the intended further processing for data subjects;

   (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

¿Usos compatibles?

PRINCIPIOS BÁSICOS

Finalidad limitada

- Finalidad "**elástica**" = consentimiento **nulo**
- Finalidad específica: sólo pueden tratarse los datos para fines **compatibles**
- Finalidad específica: sólo pueden tratarse durante el **tiempo limitado** en que ésta siga en vigor
- Finalidad específica: sólo pueden tratarse los **datos necesarios** para esa finalidad

PRINCIPIOS BÁSICOS

Proporcionalidad

- Minimización de datos en relación con la finalidad específica
- Retención de datos limitada
- Derecho al olvido

PRINCIPIOS BÁSICOS

Calidad

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

PRINCIPIOS BÁSICOS

Seguridad

Medidas técnicas y organizativas adecuadas para evitar accesos, alteraciones o usos no autorizados (confidencialidad, integridad, disponibilidad y capacidad de recuperación) en función de los riesgos y del estado del arte de la técnica

Ej.: encriptación, pseudoanonimización

PRINCIPIOS BÁSICOS

Decisiones automatizadas

(71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision -making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax -evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child. In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision -making and profiling based on special categories of personal data should be allowed only under specific conditions.

General Data Protection Regulation

PRINCIPIOS BÁSICOS

Cookies

«3. Los Estados miembros velarán por que únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE. Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de que el proveedor de un servicio de la sociedad de la información preste un servicio expresamente solicitado por el abonado o el usuario.».

https://www.boe.es/doue/2009/337/L00011-00036.pdf

PRINCIPIOS BÁSICOS

Datos de localización

Derechos de abonados y usuario de servicios de comunicaciones electrónicas:

> d) A que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado.
>
> http://www.boe.es/buscar/act.php?id=BOE-A-2003-20253

PRINCIPIOS BÁSICOS

Privacy-by-design and privacy-by-default

Article 25 - Data protection by design and by default

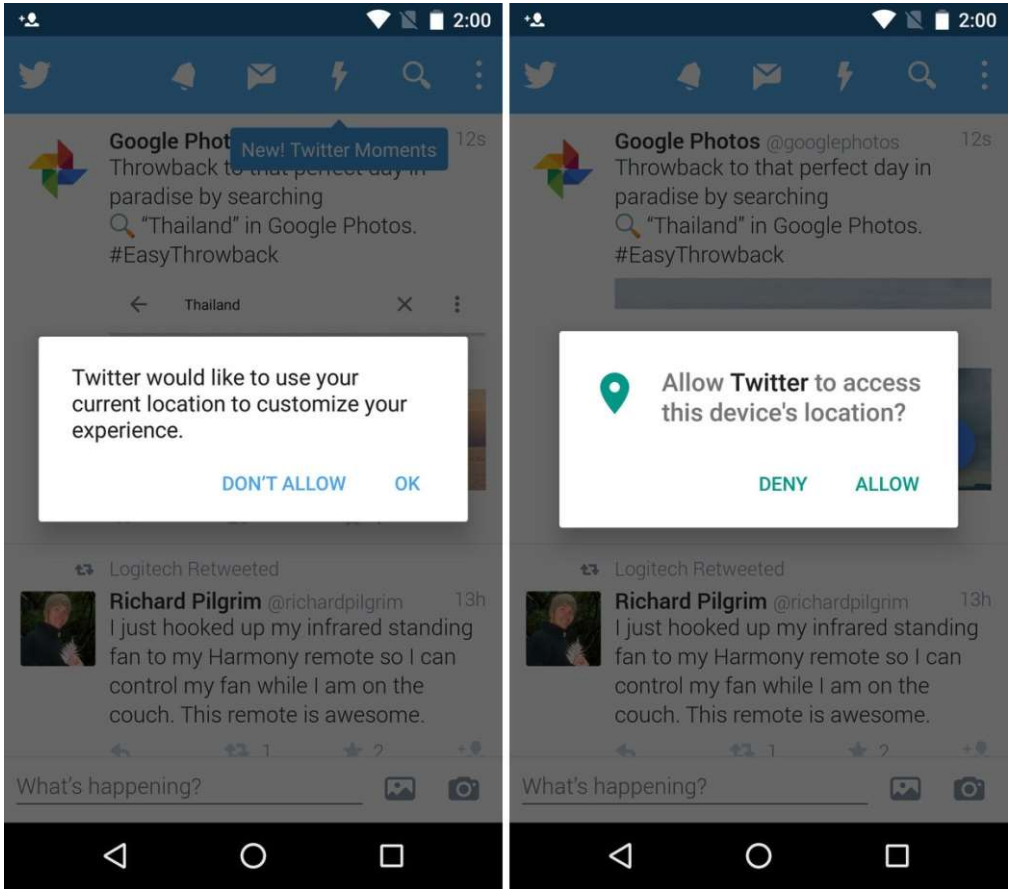
1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data -protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

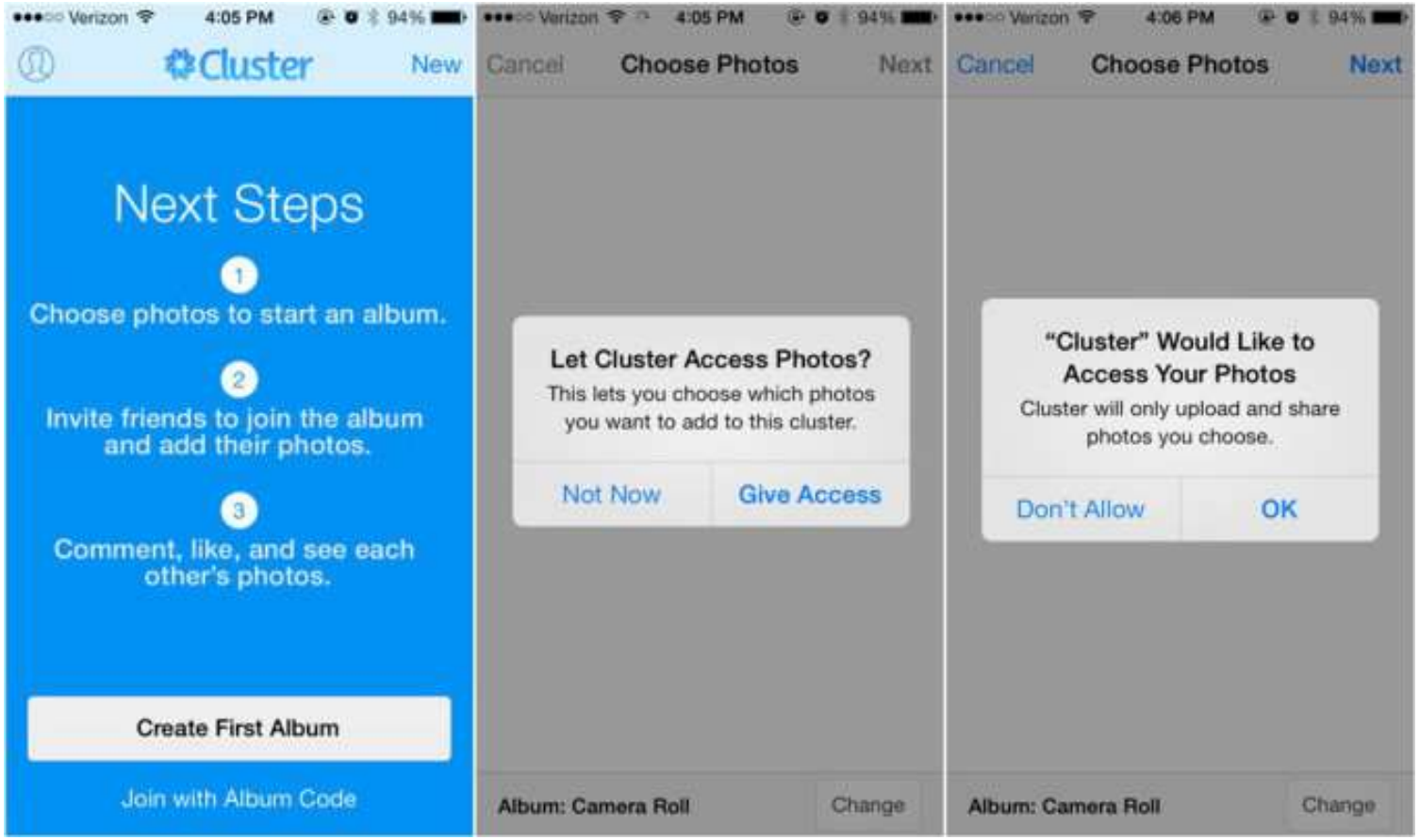
PRINCIPIOS BÁSICOS

Privacy-by-design and privacy-by-default



PRINCIPIOS BÁSICOS

Privacy-by-design and privacy-by-default



PRINCIPIOS BÁSICOS

Privacy impact assessment

Article 35 - Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

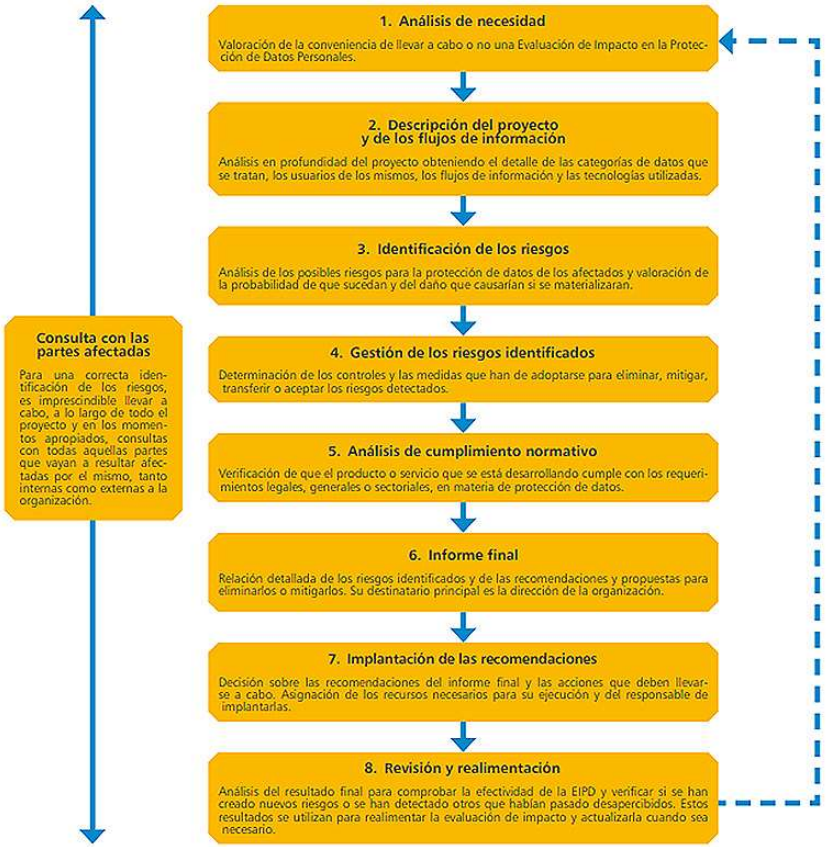
   (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

   (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

   (c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

FASES PRINCIPALES DE UNA EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS



IMPLICACIONES DE PROTECCIÓN DE DATOS PERSONALES

IMPLICACIONES EN DATOS PERSONALES

Dignidad (1)

Discriminación, segregación y exclusión

According to EPIC, in comments last April to the U.S. Office of Science and Technology Policy, "The use of predictive analytics by the public and private sector … can now be used by the government and companies to make determinations about our ability to fly, to obtain a job, a clearance, or a credit card. The use of our associations in predictive analytics to make decisions that have a negative impact on individuals directly inhibits freedom of association."

Herold, in a post on SecureWorld, noted that while overt discrimination has been illegal for decades, Big Data analytics can make it essentially "automated," and therefore more difficult to detect or prove.

IMPLICACIONES EN DATOS PERSONALES

Dignidad (2)

Invasión de la intimidad

But in addition to that, there are numerous reports of Big Data analytics being used to expose personal details, such as beginning to market products to a pregnant woman before she had told others in her family. The same can be true of things like sexual orientation or an illness like cancer.

http://www.csoonline.com/article/2855641/big-data-security/the-5-worst-big-data-privacy-risks-and-how-to-guard-against-them.html

FEB 16, 2012 @ 11:02 AM 2,980,336 VIEWS

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Kashmir Hill
FORBES STAFF

Welcome to The Not-So Private Parts where technology & privacy collide

FULL BIO >

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target TGT -2.25%, for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.

TARGET

Target has got you in its aim

IMPLICACIONES EN DATOS PERSONALES

Dignidad (3)

La dictadura de los datos

One of the potentially most powerful uses of big data is to make predictions about what is likely to happen but has not yet happened and what we are likely to do but have not yet done. For example, big data might be used to predict a child's performance at school or an adult's susceptibility to illness or premature death, to default on credit or commit crime. Notwithstanding the potential benefits, data has been described by one commentator as the 'pollution problem of the information age'[10], with the a risk of a '**dictatorship of data**' where, according to one study by a European data protection authority, *'we are no longer judged on the basis of our actions, but on the basis of what all the data about us indicate our probable actions may be'*[11].

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf

What's Even Creepier Than Target Guessing That You're Pregnant?

By Jordan Ellenberg

305 86

It's no big deal if Netflix suggests the wrong movie to you. But in other domains, bad data is more dangerous. Think about algorithms that try to identify people with an elevated chance of being involved in terrorism, or people who are more likely than most to owe the government money. Or **the secret systems the rating agencies use** to assess the riskiness of financial assets.

Here, the mistakes have real consequences. It's creepy and bad when Target intuits that you're pregnant. But it's even creepier and worse if you're *not* pregnant—or a terrorist, or a deadbeat dad—and an algorithm, doing its business in a closed and opaque box, decides that you are.

—

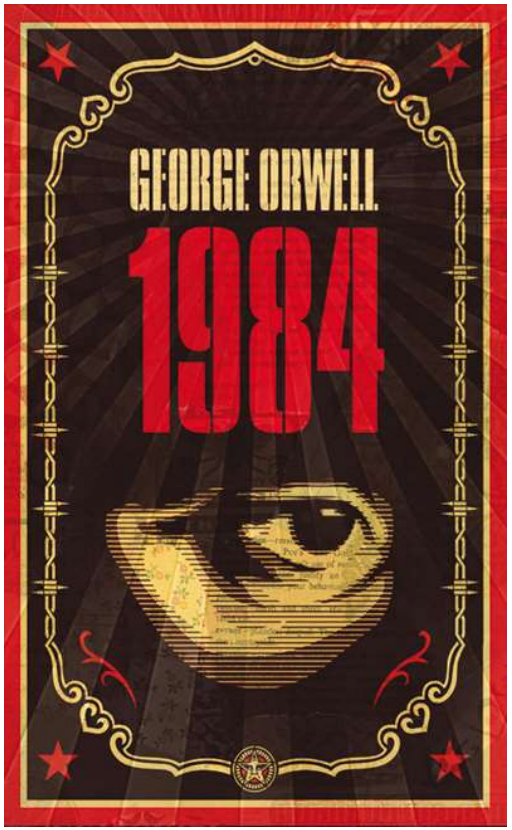
Jordan Ellenberg is a professor of mathematics at the University of Wisconsin and the author of *How Not to Be Wrong*. He blogs at Quomodocumque.

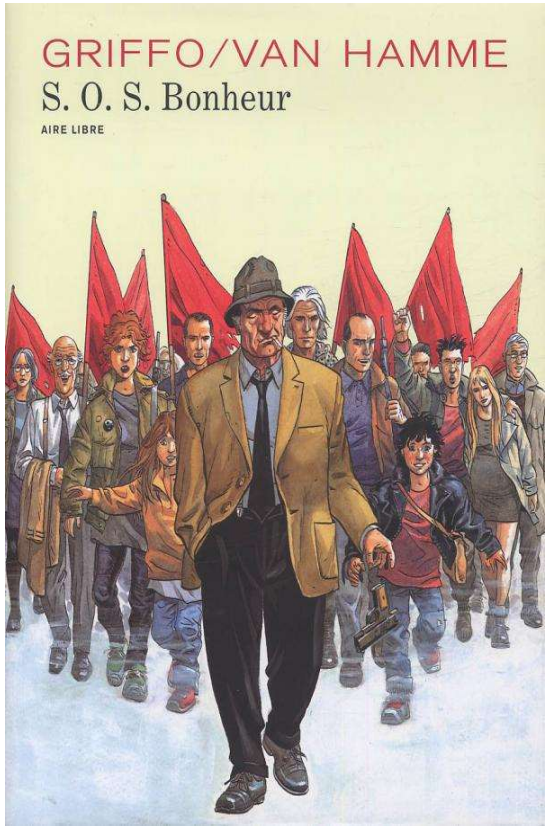
56

IMPLICACIONES EN DATOS PERSONALES

Dignidad (4)

Ataque a la libertad





Big Data Meets Big Brother: The Privacy Risks of Big Data

September 8, 2013 • Big Data & Analytics, Emerging Ideas, INNOVATION, TECHNOLOGY

By Viktor Mayer-Schönberger & Kenneth Cukier

In *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Viktor Mayer-Schönberger and Kenneth Cukier consider the benefits and threats of a big data world. In the excerpt below, the authors outline the privacy risks of big data, revealing how the value of information no longer resides solely in its primary purpose, and analysing the implications of a world in which more data is being collected and stored about each one of us than ever before.

For almost forty years, until the Berlin wall came down in 1989, the east German state security agency known as the Stasi spied on millions of people. Employing around a hundred thousand full-time staff, the Stasi watched from cars and streets. It opened letters and peeked into bank

IMPLICACIONES EN DATOS PERSONALES

Dignidad (4)

Ataque a la libertad

Big data analytics are used to identify behaviour which statistically speaking poses less risk to generates more value for organisations processes the data. There is a tendency to discourage or penalise spontaneity, experimentation or deviation from the statistical 'norm', and to reward conformist behaviour. For example, the banking and insurance sectors have an obvious interest in acquiring granular insights into the risk posed by an individual which might be revealed by combinations of datasets generated by activity on social media and by connected devices tracking location and other personal information data and the increasing number of connected objects. The need for a loan or insurance could nudge or coerce individuals into avoiding contact with certain people or companies or visiting areas with high crime rates the same way as it makes people installing 'black boxes' which allows external controller to monitor them while they are driving[13].

The very fact that our behaviour is constantly tracked and analysed may also caution us to watch how we behave and encourages us to conform, in advance, to what we perceive to be as the expected norm. These trends can also have a chilling effect on freedom of expression and other activities necessary to maintain a democratic society such as exercising the rights of free assembly or association.

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf

IMPLICACIONES EN DATOS PERSONALES

Bases legales y transparencia

In brief...

- Obtaining meaningful **consent** is often difficult in a big data context, but novel and innovative approaches can help.
- Relying on the **legitimate interests** condition is not a 'soft option'. Big data organisations must always balance their own interests against those of the individuals concerned.
- It may be difficult to show that big data analytics are strictly necessary for the performance of a **contract**.
- Big data analysis carried out in the **public sector** may be legitimised by other conditions, for instance where processing is necessary for the exercise of functions of a government department.

In brief...

- Some types of big data analytics, such as profiling, can have intrusive **effects** on individuals.
- Organisations need to consider whether the use of personal data in big data applications is within people's reasonable **expectations**.
- The complexity of the methods of big data analysis, such as machine learning, can make it difficult for organisations to be **transparent** about the processing of personal data.

IMPLICACIONES EN DATOS PERSONALES

Bases legales y transparencia

61. The Royal Academy of Engineering looked at the benefits of big data analytics in several sectors, and the risks to privacy. In the health sector, they suggested that in cases where personal data is being used with consent and anonymisation is not possible, consent could be time limited so that the data is no longer used after the time limit has expired[67]. This is in addition to the principle that, if people have given consent, they can also withdraw it at any time. They said that when seeking consent, the government and the NHS should take a patient-centric approach and explain the societal benefits and the effect on privacy.

IMPLICACIONES EN DATOS PERSONALES

Finalidad limitada

In brief...

- The purpose limitation principle does not necessarily create a barrier for big data analytics, but it means an **assessment of compatibility** of processing purposes must be done.
- **Fairness** is a key factor in determining whether big data analysis is incompatible with the original processing purpose.

80. The Opinion sets out a detailed approach to assessing whether any further processing is for an incompatible purpose. It also addresses directly the issue of repurposing data for big data analytics. It identifies two types of further processing: first, where it is done to detect trends or correlations; and second, where it is done to find out about individuals and make decisions affecting them. In the first case, it advocates a clear functional separation between the analytics operations. In the second, it says that "free, specific, informed and unambiguous 'opt-in' consent would almost always be required, otherwise further use cannot be considered compatible"[85]. It also emphasises the need for transparency, and for allowing people to correct and update their profiles and to access their data in a portable, user-friendly and machine-readable format.

IMPLICACIONES EN DATOS PERSONALES

Minimización de datos

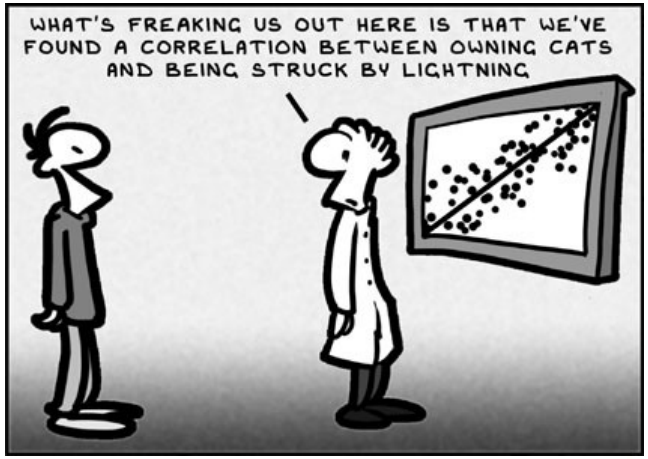
In brief...

- Big data analytics can result in the collection of personal data that is **excessive** for the processing purpose.
- Organisations may be encouraged to **retain** personal data for longer than necessary because big data applications are capable of analysing large volumes of data.

"Finding the correlation does not retrospectively justify obtaining the data in the first place. (…) Organisations therefore need to be able to articulate at the outset why they need to collect and process particular datasets. They need to be clear about what they expect to learn or be able to do by processing that data, and thus satisfy themselves that the data is relevant and not excessive, in relation to that aim. The challenge is to define the purposes of the processing and establish what data will be relevant."

IMPLICACIONES EN DATOS PERSONALES

Datos veraces



In brief…

- There are implications regarding the **accuracy** of personal data at all stages of a big data project: collection, analysis and application.
- Results of data analysis may not be **representative** of the population as a whole.
- **Hidden biases** in datasets can lead to inaccurate predictions about individuals.

"Data quality is a key issue for organisations using big data analytics. This is linked to what is often seen as the 'fourth V' of big data: veracity, or in other words the reliability of the data. Senior managers in big data organisations need to know whether they can trust what the data is apparently telling them."

Information governance issue	Data protection provision
Security and monitoring	Principle 7 – security
Protection and masking of sensitive data	Sensitive data definition and conditions for processing
Profiling data sources (lineage, traceability, format, etc.)	Anonymisation and definition of personal data; Principle 1 – fairness
Data lifecycle management: archiving data	Principle 5 – retention

IMPLICACIONES EN DATOS PERSONALES

Derechos de los individuos

In brief...

- The vast quantities of data used in big data analytics may make it more difficult for organisations to comply with the **right of access** to personal data.
- Organisations will need to have appropriate processes in place to deal with the GDPR's extension of rights regarding **decisions based on automated processing.**

- Right of access: right to receive a "copy" (in a commonly used electronic form is the request is made electronically) as well as information about its sources.
- Right not be subject to an automated decision which significantly affects the individuals.
- Right to be forgotten: "It may be practically difficult for a business to find and erase someone's data if it is stored across several different systems."

IMPLICACIONES EN DATOS PERSONALES

Seguridad (1)

In brief...

- There are several **information security risks** specific to big data analytics.
- Organisations need to recognise these new risks and put in place **appropriate security measures.**

"ENISA produces a regular report on the big data 'threat landscape'. The latest report recognised that big data analytics can be a powerful tool in detecting security risks, but it also identified several potential security risks specific to big data processing. For example, the high level of replication in big data storage and the frequency of outsourcing the analytics increase the risk of breaches, data leakages and degradation; also, the creation of links between the different datasets could increase the impact of breaches and leakages. In a further study, (…) threats to do with access controls, the ability to securely restore datasets, and validation of the data sources."

IMPLICACIONES EN DATOS PERSONALES

Seguridad (2)

Data Security

This risk is obvious and often uppermost in our minds when we are considering the logistics of data collection and analysis. Data theft is a rampant and growing area of crime – and attacks are getting bigger and more damaging. In fact five of the six most damaging data thefts of all time (eBay, JP Morgan Chase, Adobe, Target, and Evernote) were carried out within the last two years.

The bigger your data, the bigger the target it presents to criminals with the tools to steal and sell it. In the case of Target, hackers stole credit and debit card information of 40 million customers, as well as personal identifying information such as email and geographical addresses of up to 110 million people. In March, a federal judge approved a settlement in which Target would pay $10 million into a settlement fund, from which payments of up to $10,000 would be made to everyone affected by the breach.

http://data-informed.com/the-5-biggest-risks-of-big-data/

IMPLICACIONES EN DATOS PERSONALES

Accountability

In brief...

- Accountability is increasingly important for big data analytics and will become an explicit **requirement under the GDPR.**
- Big data organisations may need to make **changes** to their reporting structures, internal record keeping and resource allocation.
- Machine learning algorithms have the potential to make decisions that are **discriminatory**, **erroneous** and **unjustified.**
- **Data quality** is a key issue for those with information governance responsibilities in a big data context.

- Records: in a big data context, the initial analysis of data is often experimental and without any predefined hypothesis or business need.
- DPO mandatory for any systematic monitoring of individuals on a large scale.
- Algorithmic accountability: to check that the algorithms used and developed by machine learning systems are actually doing what we think they are doing and are not producing discriminatory, erroneous or unjustified results.

IMPLICACIONES EN DATOS PERSONALES

Responsables y encargados

In brief...

- Big data analytics can make it **difficult to distinguish** between **data controllers** and **data processors.**
- Organisations **outsourcing** analytics to companies specialising in AI and machine learning need to consider carefully who has **control** over the processing of any personal data.

"If that company has enough freedom to use its expertise to decide what data to collect and how to apply its analytic techniques, it is likely to be a data controller as well. For instance, in a forthcoming article on the transfer of data from the Royal Free London NHS Foundation Trust to Google DeepMind, Julia Powles argues that, despite assertions to the contrary, DeepMind is actually a joint data controller as opposed to a data processor".


Google DeepMind and healthcare in an age of algorithms

Authors | Authors and affiliations

Julia Powles, Hal Hodson

Open Access | Original Paper

First Online: 16 March 2017

Cite this article as: Powles, J. & Hodson, H. Health Technol. (2017). doi:10.1007/s12553-017-0179-1

628 Shares | 19k Downloads

http://rd.springer.com/article/10.1007/s12553-017-0179-1

HERRAMIENTAS (¿REALISTAS?)
DE PROTECCIÓN DE DATOS

HERRAMIENTAS (¿REALISTAS?) DE CUMPLIMIENTO

Anonimización y privacidad por el diseño (1)

In brief...

- The benefits of big data need not come at the cost of privacy.
- Embedding **privacy by design** solutions into big data analytics can help to protect privacy through a range of technical and organisational measures.
- Under the **GDPR**, privacy by design – known as **'data protection by design and by default'** – will become a **legal requirement**.

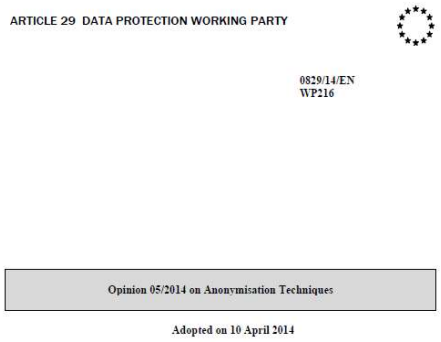
In brief...

- Often, big data analytics will not require the use of data that identifies individuals.
- **Anonymisation** can be a successful tool that takes processing out of the data protection sphere and mitigates the risk of loss of personal data.
- Organisations using anonymisation techniques need to make robust assessments of the **risk of re-identification**.

- **Data protection and privacy by design**
  - ❑ Privacy-conscious engineering
  - ❑ Separación funcional
  - ❑ Anonimización

HERRAMIENTAS (¿REALISTAS?) DE CUMPLIMIENTO

Anonimización y privacidad por el diseño (2)

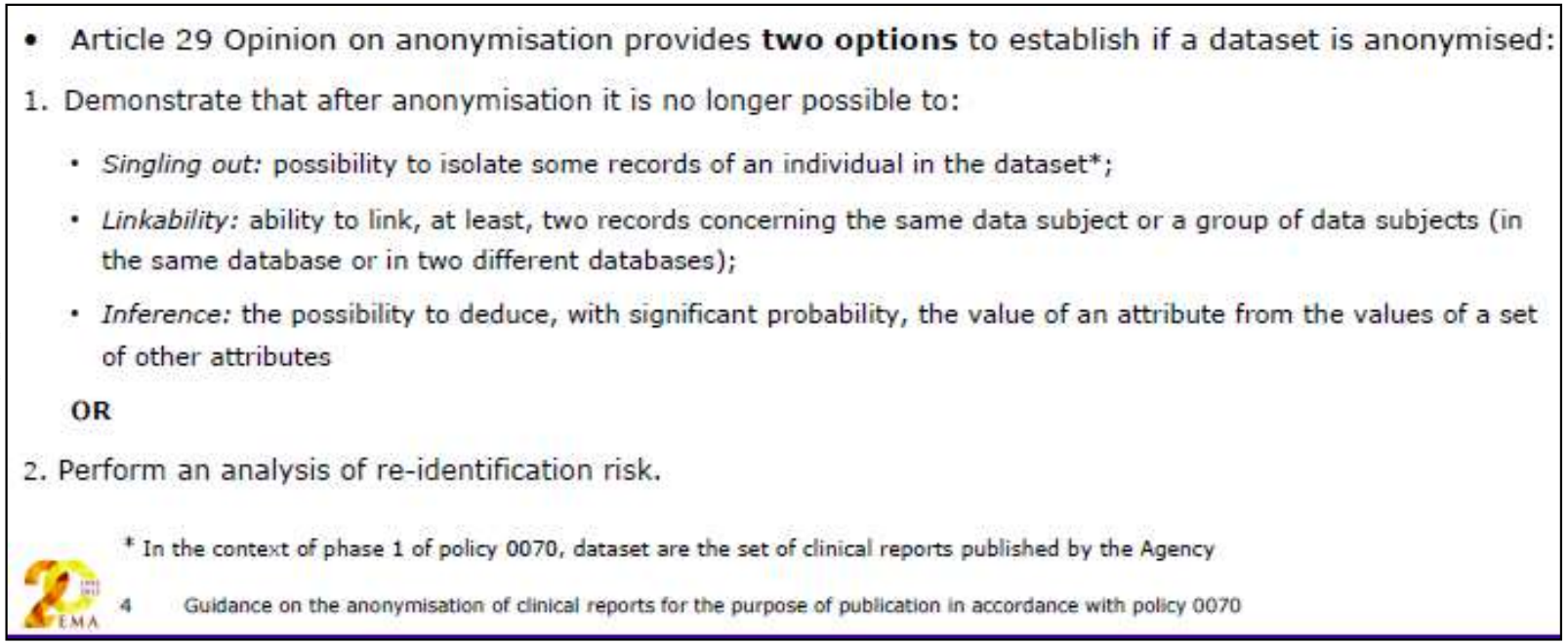

ARTICLE 29 DATA PROTECTION WORKING PARTY

0829/14/EN
WP216

Opinion 05/2014 on Anonymisation Techniques

Adopted on 10 April 2014

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf


- Article 29 Opinion on anonymisation provides **two options** to establish if a dataset is anonymised:

1. Demonstrate that after anonymisation it is no longer possible to:
   - *Singling out:* possibility to isolate some records of an individual in the dataset*;
   - *Linkability:* ability to link, at least, two records concerning the same data subject or a group of data subjects (in the same database or in two different databases);
   - *Inference:* the possibility to deduce, with significant probability, the value of an attribute from the values of a set of other attributes

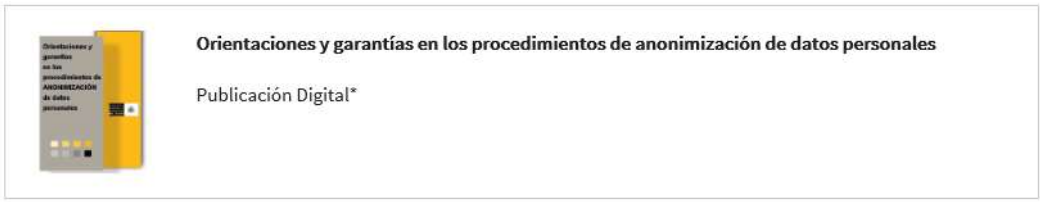
OR

2. Perform an analysis of re-identification risk.

* In the context of phase 1 of policy 0070, dataset are the set of clinical reports published by the Agency

http://www.ema.europa.eu/docs/en_GB/document_library/Presentation/2015/06/WC500188859.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS


Orientaciones y garantías en los procedimientos de anonimización de datos personales

Publicación Digital*

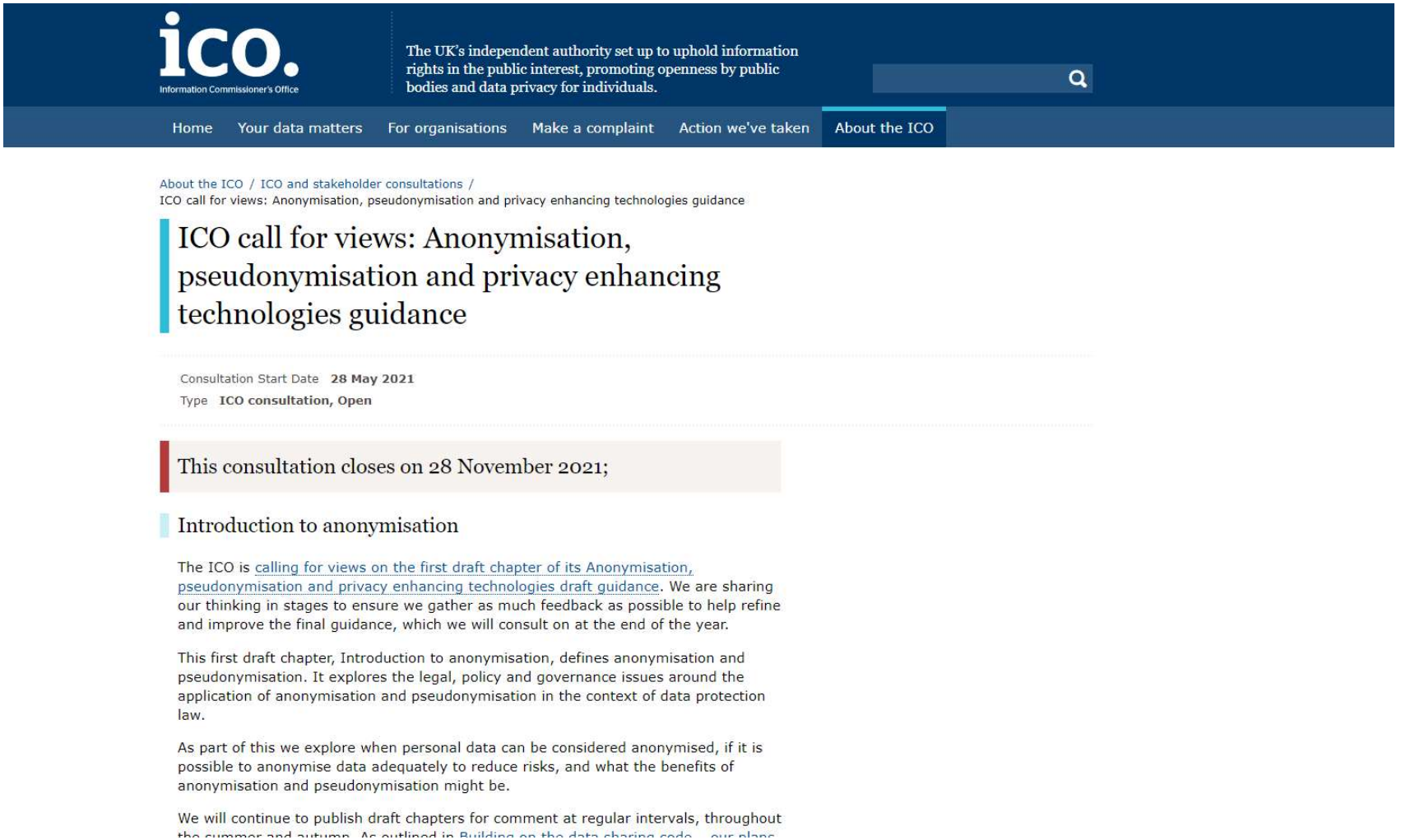
Orientaciones sobre protección de datos en la reutilización de la información del sector público

Publicación Digital*

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.phphttp://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php

HERRAMIENTAS (¿REALISTAS?) DE CUMPLIMIENTO

Anonimización y privacidad por el diseño (3)



ico.
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home | Your data matters | For organisations | Make a complaint | Action we've taken | About the ICO

About the ICO / ICO and stakeholder consultations /
ICO call for views: Anonymisation, pseudonymisation and privacy enhancing technologies guidance

ICO call for views: Anonymisation, pseudonymisation and privacy enhancing technologies guidance

Consultation Start Date **28 May 2021**
Type **ICO consultation, Open**

This consultation closes on 28 November 2021;

Introduction to anonymisation

The ICO is calling for views on the first draft chapter of its Anonymisation, pseudonymisation and privacy enhancing technologies draft guidance. We are sharing our thinking in stages to ensure we gather as much feedback as possible to help refine and improve the final guidance, which we will consult on at the end of the year.

This first draft chapter, Introduction to anonymisation, defines anonymisation and pseudonymisation. It explores the legal, policy and governance issues around the application of anonymisation and pseudonymisation in the context of data protection law.

As part of this we explore when personal data can be considered anonymised, if it is possible to anonymise data adequately to reduce risks, and what the benefits of anonymisation and pseudonymisation might be.

We will continue to publish draft chapters for comment at regular intervals, throughout the summer and autumn. As outlined in Building on the data sharing code – our plans

HERRAMIENTAS (¿REALISTAS?) DE CUMPLIMIENTO

Accountability (1)

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 7/2015

Meeting the challenges of big data

Some of the key decisions an accountable organisation must make under European data protection law include:

- whether any secondary use of data complies with the principle of purpose limitation,
- whether data initially used in one context can be considered adequate, relevant, and proportionate to be reused in another context, and
- whether, in the absence of obtaining consent from the individuals, an organisation can rely on its legitimate interest to process any data.

While these assessments are based on legal requirements, they often require a comprehensive balancing exercise and consideration of many factors, including whether the data processing meets the reasonable expectations of the individuals concerned, whether it may lead to unfair discrimination or may have any other negative impact on the individuals concerned or on society as a whole. These assessments often raise challenging questions of business ethics and fairness, and cannot be reduced to a simple and mechanical exercise of ticking off compliance boxes. The more powerful computers become, the more acute is the challenge: for example, research has found that computers are more accurate than humans at predicting from 'digital footprints' personality traits, political attitudes and physical health [45].

For these reasons, such assessments may be best tackled by a multidisciplinary group (e.g. computer scientists, engineers, lawyers, data protection officers, statisticians, data scientists, doctors, scientists, marketing, insurance or finance specialists)

HERRAMIENTAS (¿REALISTAS?) DE CUMPLIMIENTO

Accountability (2)

Summary of Research Considerations

In light of this research, companies already using or considering engaging in big data analytics should:

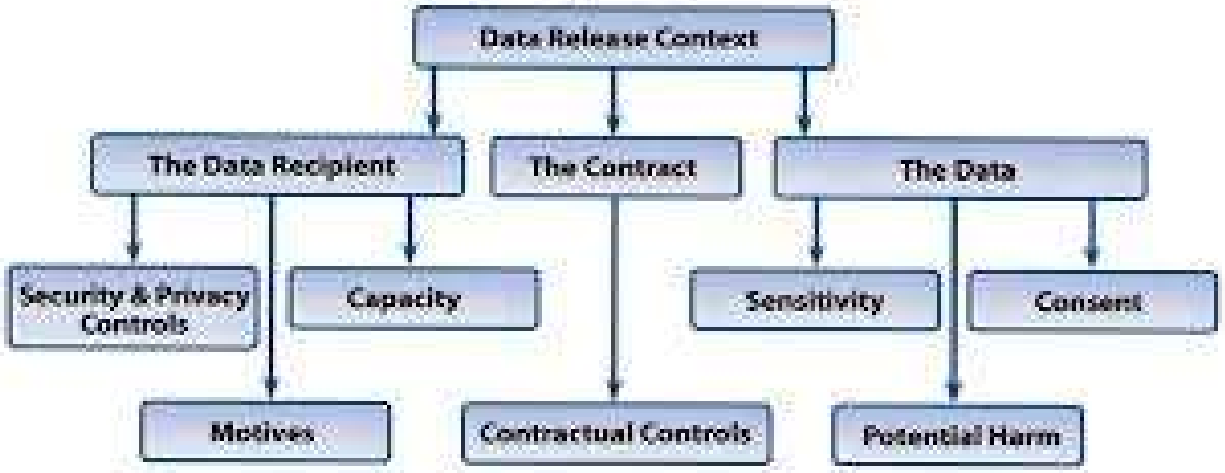
- Consider whether your data sets are missing information from particular populations and, if they are, take appropriate steps to address this problem.
- Review your data sets and algorithms to ensure that hidden biases are not having an unintended impact on certain populations.
- Remember that just because big data found a correlation, it does not necessarily mean that the correlation is meaningful. As such, you should balance the risks of using those results, especially where your policies could negatively affect certain populations. It may be worthwhile to have human oversight of data and algorithms when big data tools are used to make important decisions, such as those implicating health, credit, and employment.
- Consider whether fairness and ethical considerations advise against using big data in certain circumstances. Consider further whether you can use big data in ways that advance opportunities for previously underrepresented populations.

HERRAMIENTAS (¿REALISTAS?) DE CUMPLIMIENTO

Accountability (3)

In brief...

- A **privacy impact assessment** is an important tool that can help to **identify and mitigate privacy risks** before the processing of personal data.
- Under the **GDPR**, it is highly likely that doing a privacy impact assessment – known as a **'data protection impact assessment'** – will be a **requirement** for big data analytics involving the processing of personal data.
- The unique features of big data analytics can make some steps of a privacy impact assessment more **difficult**, but these **challenges** can be **overcome**.



HERRAMIENTAS (¿REALISTAS?) DE CUMPLIMIENTO

El papel de la ética (1)

In brief...

- An **ethical approach** to the processing of personal data in a big data context is a very **important compliance tool.**
- **Ethics boards** at organisational and national level can help to assess issues and ensure the application of ethical principles.
- Ethical approaches to the use of personal data can help to build **trust** with individuals.
- There is a role for the setting of **big data standards** to encourage best practice across industries.

Prof. Dr. Christiane Woopen
Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health
University of Cologne

Ethical Challenges related to big data

- Autonomy and Consent
  - Can we introduce the concept of broad consent?
  - Big data may also help to finally get rid of paternalism (E.Topol)
- Privacy and Confidentiality
  - Meaning of anonimity?
  - Treaty on data protection?
- Justice
  - Only for the happy few? Or for all, using telemedicine?
- Condition Humaine
  - Permanent observation/ control (cf Bentham's panopticum)

HERRAMIENTAS (¿REALISTAS?) DE CUMPLIMIENTO

El papel de la ética (2)

'Human dignity is inviolable. It must be respected and protected.'

Article 1, EU Charter of Fundamental Rights

The fundamental rights to privacy and to the protection of personal data have become more important for the protection of human dignity than ever before. They are enshrined in the EU Treaties and in the EU Charter of Fundamental Rights. They enable individuals to develop their own personalities, to lead independent lives, to innovate and to exercise other rights and freedoms. The data protection principles defined in the EU Charter -necessity, proportionality, fairness, data minimisation, purpose limitation, consent and transparency- apply to data processing in its entirety, to collection as well as to use.

Technology should not dictate values and rights, but neither should their relationship be reduced to a false dichotomy. The digital revolution promises benefits for health, the environment, international development and economic efficiency. Under the EU's plans for a digital single market, cloud computing, the 'Internet of Things', big data and other technologies are considered key to competitiveness and growth. Business models are exploiting new capabilities for the massive collection, instantaneous transmission, combination and reuse of personal information for unforeseen purposes, and justified by long and impenetrable privacy policies. This has placed the principles of data protection under new strains, which calls for fresh thinking on how they are applied.

In today's digital environment, adherence to the law is not enough; we have to consider the ethical dimension of data processing. The EU's regulatory framework already allows room for flexible, case-by-case, decisions and safeguards when handling personal information. The reform of the regulatory framework will be a good step forward. But there are deeper questions as to the impact of trends in data driven society on dignity, individual freedom and the functioning of democracy.

These issues have engineering, philosophical, legal and moral implications. This Opinion highlights some major technology trends which may involve unacceptable processing of personal information or may interfere with the right to privacy. It outlines a four-tier 'big data protection ecosystem' to respond to the digital challenge: a collective effort, underpinned by ethical considerations.

(1) Future-oriented regulation of data processing and respect for the rights to privacy and to data protection.

(2) Accountable controllers who determine personal information processing.

(3) Privacy conscious engineering and design of data processing products and services.

(4) Empowered individuals.

The European Data Protection Supervisor wants to stimulate an open and informed discussion in and outside the EU, involving civil society, designers, companies, academics, public authorities and regulators. The new EU data protection ethics board we will establish at the EDPS will help define a new digital ethics, allowing to realise better the benefits of technology for society and the economy in ways which reinforce the rights and freedoms of individuals.

HERRAMIENTAS (¿REALISTAS?) DE CUMPLIMIENTO

Transparencia (1)

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 7/2015

Meeting the challenges of big data

- **Transparency: end covert profiling**

  - ❑ Disclosing the logic involved in Big Data analytics
  - ❑ Better tools for informing individuals

- **Beyond unreadable privacy policies**

- ❑ **Short of consent: right to object and opt-out mechanisms**
- ❑ **Beyond consent: user control and sharing the benefits**
  - Right of access and data portability
  - Personal data spaces
- ❑ **New, innovative ways to provide information, access and control to individuals**

HERRAMIENTAS (¿REALISTAS?) DE CUMPLIMIENTO

Transparencia (2)

Questions for Legal Compliance

In light of these existing laws, companies already using or considering engaging in big data analytics should, among other things, consider the following:

- If you compile big data for others who will use it for eligibility decisions (such as credit, employment, insurance, housing, government benefits, and the like), are you complying with the accuracy and privacy provisions of the FCRA? FCRA requirements include requirements to (1) have reasonable procedures in place to ensure the maximum possible accuracy of the information you provide, (2) provide notices to users of your reports, (3) allow consumers to access information you have about them, and (4) allow consumers to correct inaccuracies.
- If you receive big data products from another entity that you will use for eligibility decisions, are you complying with the provisions applicable to users of consumer reports? For example, the FCRA requires that entities that use this information for employment purposes certify that they have a "permissible purpose" to obtain it, certify that they will not use it in a way that violates equal opportunity laws, provide pre-adverse action notice to consumers, and thereafter provide adverse action notices to those same consumers.
- If you are a creditor using big data analytics in a credit transaction, are you complying with the requirement to provide statements of specific reasons for adverse action under ECOA? Are you complying with ECOA requirements related to requests for information and record retention?
- If you use big data analytics in a way that might adversely affect people in their ability to obtain credit, housing, or employment:
  - Are you treating people differently based on a prohibited basis, such as race or national origin?
  - Do your policies, practices, or decisions have an adverse effect or impact on a member of a protected class, and if they do, are they justified by a legitimate business need that cannot reasonably be achieved by means that are less disparate in their impact?
- Are you honoring promises you make to consumers and providing consumers material information about your data practices?
- Are you maintaining reasonable security over consumer data?
- Are you undertaking reasonable measures to know the purposes for which your customers are using your data?
  - If you know that your customer will use your big data products to commit fraud, do not sell your products to that customer. If you have reason to believe that your data will be used to commit fraud, ask more specific questions about how your data will be used.
  - If you know that your customer will use your big data products for discriminatory purposes, do not sell your products to that customer. If you have reason to believe that your data will be used for discriminatory purposes, ask more specific questions about how your data will be used.

HERRAMIENTAS (¿REALISTAS?) DE CUMPLIMIENTO

Transparencia (3)

In brief...

- There are several **innovative approaches to providing privacy notices** including the use of videos, cartoons, just-in-time notifications and standardised icons.
- Using a **combination of approaches** can help make complex information on big data analytics easier to understand.

In brief...

- **Auditing techniques** can be used to identify the factors that influence an algorithmic decision.
- **Interactive visualisation systems** can help individuals to understand why a recommendation was made and give them control over future recommendations.
- **Ethics boards** can be used to help shape and improve the transparency of the development of machine learning algorithms.
- A **combination of technical and organisational approaches** to algorithmic transparency should be used.

HERRAMIENTAS (¿REALISTAS?) DE CUMPLIMIENTO

Transparencia (4)

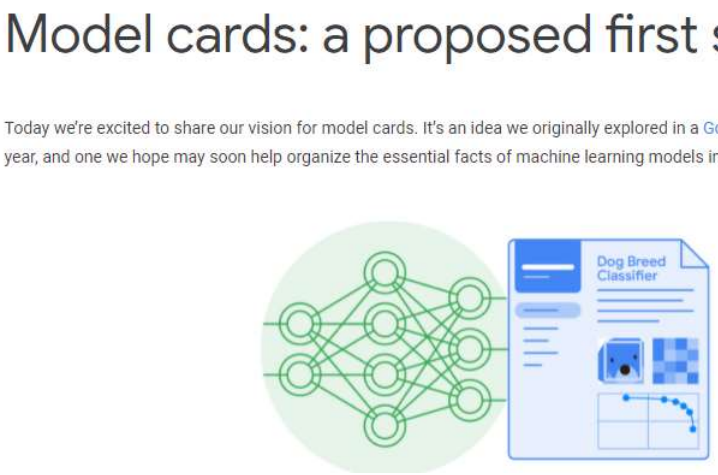
Dynamic consent, the concept

- based on participation and transparency
- initial broad consent from the participant
- continuous update on the specific use of data
- individual can opt out from specific uses of data while allowing the use for other purposes
- requires education and information
- empowering individuals to shape the possibilities of research by 'voting' for those uses
- project becomes a shared or joint enterprise of the individual along with the researcher
- Conditions: some amount of health literacy, time, internet connectivity (scientific citizenship)

HERRAMIENTAS (¿REALISTAS?) DE CUMPLIMIENTO

Transparencia (5)

[Google AI Blog: Introducing the Model Card Toolkit for Easier Model Transparency Reporting (googleblog.com)]

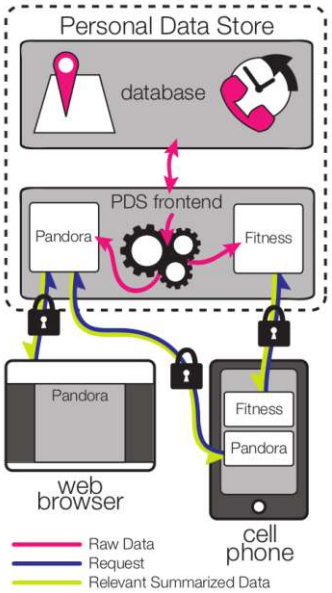


HERRAMIENTAS (¿REALISTAS?) DE CUMPLIMIENTO

Personal data stores

In brief...

- The use of personal data stores can address issues of fairness and lack of transparency by giving individuals **greater control** over their personal data.
- Personal data stores can support the concept of **data portability** (which will become law under the GDPR in certain conditions) regarding the re-use of an individual's personal data under their control.



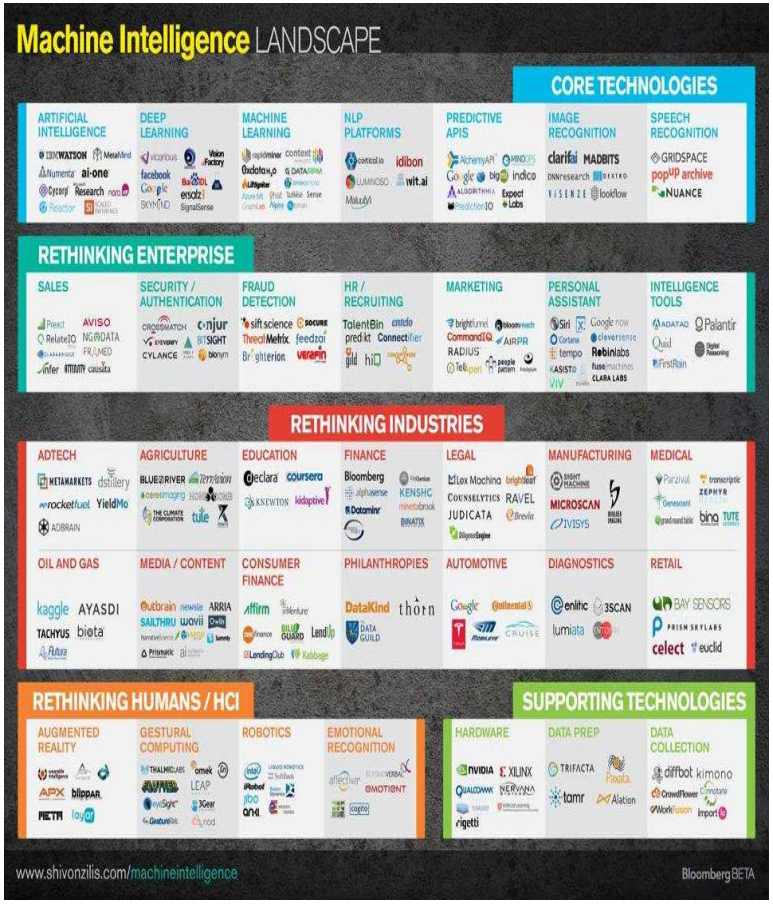
http://openpds.media.mit.edu/#architecture

Sellos y certificaciones de privacidad

In brief...

- **Certification schemes** can be used to help demonstrate the data protection compliance of big data processing operations.
- The **GDPR** will encourage the establishment of such schemes.

REFLEXIONES FINALES



- Definition of AI
- Horizontal or sectorial regulation?
- Fairness
- Benefits of AI
- Ex-Ante check
- Transparency and explainability
- Quality and traceability
- Risk
- Facial Recognition
- Liability
- Auditability

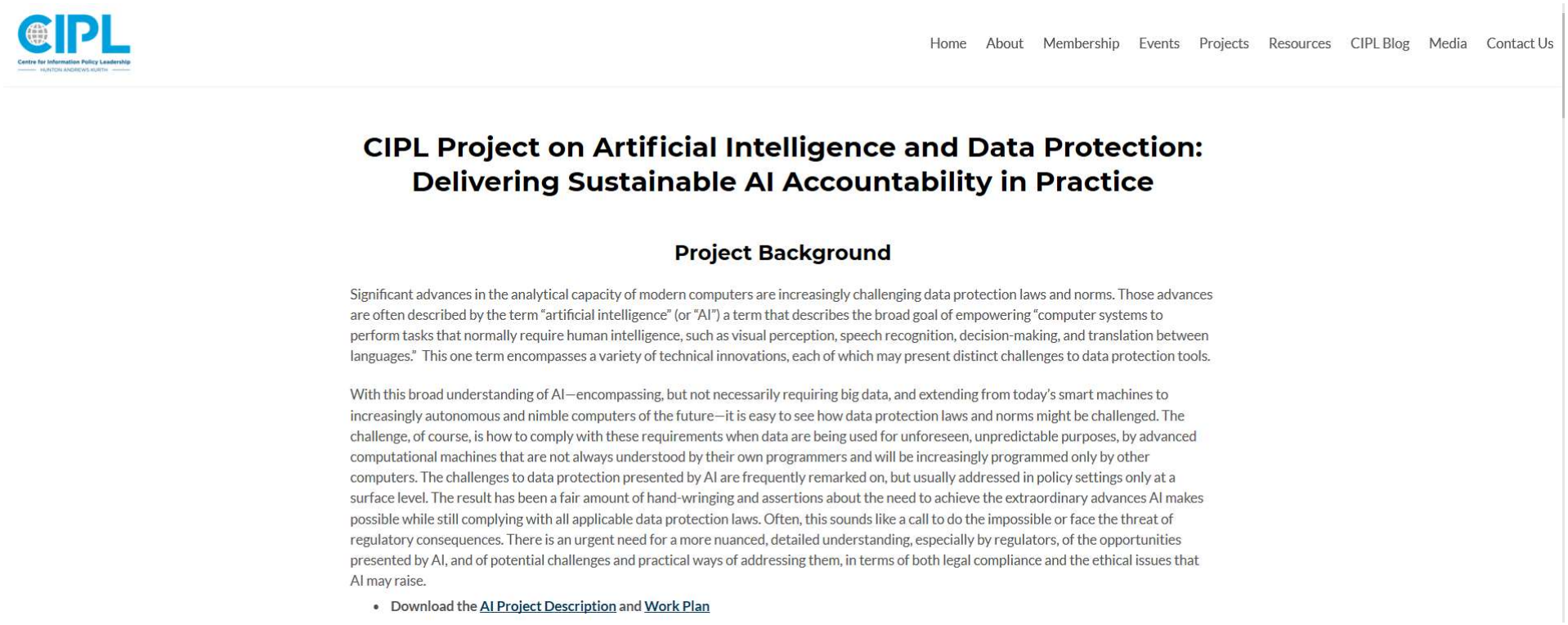
REFLEXIONES FINALES

AI is not good or bad, nor is it neutral | Lokke Moerel | TEDxAmsterdamWomen

4,451 views 30 6 SHARE SAVE

https://www.youtube.com/watch?v=HPyHf4IWDQc

REFLEXIONES FINALES



https://www.informationpolicycentre.com/ai-project.html

REFLEXIONES FINALES

EURACTIV The Capitals The Brief Ukraine

Agrifood | Economy & Jobs | Energy & Environment | Global Europe | Health | Politics | Technology | Transport | Brussels

AI standards set for joint drafting among European standardisation bodies

By Luca Bertuzzi | EURACTIV.com

May 30, 2022

Type here to search

24°C 10:28 AM 01-Jun-22


Q&A