1. Algorithms challenge the banking industry

Algorithms become a competitive asset for banks, demanding stronger ways of protection to foster innovation

Algorithms are at the core of data analytics, the foundation on which forward thinking societies are built. The digital transformation of the economy and the development of new platform ecosystems also rely heavily on them. Data-driven organizations, such as financial institutions, require appropriate and stronger ways of protecting algorithms, as they are part of the organizations know how. Besides, ethics and transparency become key considerations in their design.

Abstract

In the financial services industry, algorithms are intensively used for various purposes, from offering more personalised finance products due to data analytics based in algorithms to improving areas like investment analysis, risk assessment, fraud prevention or trading. The overall goal of the use of algorithms is to extract value from data, for the benefit of both consumers and organizations. Algorithms, as a competitive asset for banks, need stronger ways of protection to drive value creation and foster innovation for the delivery of new products, services and processes. Avoiding discrimination and transparency on the use of algorithms also becomes a must for banks. The new General Data Protection Regulation (GDPR) is a relevant rule that promotes transparency while reinforces the rights of individuals in relation to data protection and automated decision making.

Know how protection to foster innovation

Algorithms allow for higher quality services as well as better decision making, for the benefit of both consumers and enterprises. For this reason, the legal framework under which algorithms operate should not limit their innovative potential but reinforce it. Algorithms protection becomes essential for all data driven organizations, while maximizing the economic value of an algorithmic asset critically depends on understanding the nature of the intellectual property rights involved and how best to use the available forms of protection.

As for the way to legally protect algorithms, there is no copyright or industrial property law explicitly referred to algorithm protection. Moreover, algorithm protection varies depending on the jurisdiction. There are several mechanisms of protection to be considered: patents, copyright, know how protection or industrial secrecy.

There has been much debate as to whether algorithms and computer programs are more like processes and machines, therefore eligible for patenting, or more like the laws of nature, therefore unpatentable[1]. On the other hand, patents are two-edge swords, as they confer market power on their holder and therefore limit competition. Software patents have traditionally been questioned[2]. In the EU, as for the protection through patents, there is an explicit exclusion of mathematical methods, as long as these methods are the unique

1: Maier, Gregory J.: "Software protection-integrating patent, copyright and trade secret law", *Journal of the Patent and Trademark Office Society*, vol.69, nº3, pag. 152-165,1987.
2: Study of the effects of algorithmic patent claims for computer implemented inventions, commissioned by DG Information Society of the European Commission, June 2008.

purpose of the patent[3], but this instrument can be used if the algorithm is integrated into another invention or if it is part of it. As for copyright protection, it protects the expression of ideas, methods or theories in a written work or as software. One of the important advantages of patents over copyright is that patents protect against independent developments, while copyright only protect against derivation from protected works. Therefore, a copyright applied to software would appear to protect only the intellectual property embodied in software as a mode of expression.

Many enterprises protect algorithms through industrial secrecy and know how protection. On June 2016, the Directive 2016/943 on the protection of undisclosed *know how* and business information (trade secrets) against their unlawful acquisition, use and disclosure, was adopted. As long as the algorithm has a commercial value and has been kept secret with specific measures, this Directive would offer protection against an unlawful access or disclosure and offers ways to obtain compensation for damages. This Directive is a step forward for businesses to protect their innovative work and preserve competitive gains.

Discrimination risk and supervision

An algorithm is a collection of instructions for carrying out a task, where certain inputs are transformed into outputs. They can be defined as "a mathematical method to solve a problem that consists of exactly defined instructions"[4]. Algorithms can also be defined as "a formally specified sequence of logical operations that provides step-by-step instructions for computers to act on data and, thus, automated decisions"[5]. Algorithms are helpful for both consumers and organizations but demand a proper design and monitoring. Alongside their potential benefits, big data technologies can be used to discriminate against individuals, potentially enabling discriminating outcomes, reducing opportunities and choices available to them. Therefore, there is a "need to ensure fairness in automated decisions, preserving constitutional principles, enhancing individual control over personal information, and protecting people from inaccurate data"[6]. So-called *black box* algorithms cannot guarantee such fairness, as they are basically systems in which the inner workings are mysterious, where we can observe their inputs and outputs but we cannot infer how one becomes the other[7].

In order to ensure an appropriate knowledge of how algorithms actually work, Mayer-Schönberger & Cukier (2013)[8] discuss the possibility of introducing the role of *algorithms monitors*, scientists who audit algorithms. The creation of professional bodies of algorithm monitors could be considered, with members, just like doctors, lawyers, architects and other professions, who are subject to strict conduct and ethical codes in their activities. Another idea would be to establish internal algorithm monitors within organizations to monitor *in situ* the activities being conducted with personal data, protecting in particular the interests of people who might be affected. There would be an algorithm *ombudsman* to make sure that the entire data handling process, from the moment data is obtained, up to the final outputs, is managed using ethical and scientific good practice.[9]

3: Art.52 European Patent Convention.
4: Futscher, Gerarld: *Algorithmic thinking: the key for understanding computer science*, Vienna University of Technology, Institute of Software, Technology and Interactive systems, 2006.
5: Solon Barocas et al: Data & civil rights: technology primer (2014). http://www.datacivilrights.org/pubs/2014-1030/Technology.pdf [https://perma.cc/X3YX-XHNA].
6: *Big Data: Seizing opportunities, preserving values*, White House, February, 2015, p.6.
7: Pasquale, F:"The black box society: the secret algorithms that control money and information", Harvard University Press, 2015.
8: Mayer-Schönberger, Viktor & Cukier, Kenneth: *Big Data: A revolution that will transform how we live, work and think,* Houghton Miffin Harcourt, 2013.
9: Alonso, J., Tuesta, D., Cuesta, C., and Fernandez de Lis, S.: "An approach to the economy of personal data and its regulation", Economic Watch, BBVA Research, Sept. 2014.

Algorithms also pose risks in relation to possible market distortion, collusion prices or herd behaviour risk among industry players. Regulators are beginning to grasp the implications of these powerful tools, finding ways to prevent collusion among machines. It is a relevant challenge Competition law enforcers will face[10].

GDPR and the 'right to explanation': algorithm transparency

The General Data Protection Regulation (GDPR)[11] is an ambitious regulation in the field of data protection that will be applicable from May 2018 in the European Union. As regards automated decision making (including profiling) that significantly impact data subjects, it reinforces a right to explanation of the logic of algorithms. Opacity is at the very heart of new concerns about algorithms[12]. To address it, probably widespread educational efforts would make consumers more aware about the mechanics of algorithms. "Transparency is not just an end in itself, but an interim step on the road to intelligibility"[13]. Beyond the right to obtain human intervention, to obtain an explanation of the logic and consequences of algorithms, a data subject's right to express his or her point of view and to challenge the decision, the Regulation does not specify the type of measures to be taken. What does it mean and what is required to explain an algorithmic decision? The answer to the question is not obvious. The GDPR implies a challenge for all industries, and especially for financial services firms, as data scientists will have to design efficient algorithms that can be explained in an understandable manner, striking the right balance between transparency and know how protection, avoiding a full algorithm disclosure.

Conclusion

Algorithms are fundamental elements not only for the banking industry but for all industries that are data-driven and rely on an intensive use of automated processing. Algorithms are part of the organizations' *know how* and demand stronger ways of protection. However, any enterprise that processes personal data from European residents, offering goods or services to them, has to be able to explain the logic of algorithms in automated decision making, including profiling. The GDPR is challenging data scientists, on the one hand, who must design efficient algorithms that can be easily explained and avoid discrimination, while it is also challenging the entire organization to build a strategy for a strong algorithm protection framework.

10: "*Policing the digital cartels: price-setting algorithms mean regulators must now tackle collusion among machines*", January 8th 2017, Financial Times
11: General Data Protection Regulation (679/2016).
12: Burrell, Jenna: "How the machine 'thinks': understanding opacity in machine learning algorithms", *Big Data & Society*, SAGE Journals, January 2016.
13: Pasquale, F.: *op, cit,* pag. 8.

DISCLAIMER

This document has been prepared by BBVA Research Department, it is provided for information purposes only and expresses data, opinions or estimations regarding the date of issue of the report, prepared by BBVA or obtained from or based on sources we consider to be reliable, and have not been independently verified by BBVA. Therefore, BBVA offers no warranty, either express or implicit, regarding its accuracy, integrity or correctness.

Estimations this document may contain have been undertaken according to generally accepted methodologies and should be considered as forecasts or projections. Results obtained in the past, either positive or negative, are no guarantee of future performance.

This document and its contents are subject to changes without prior notice depending on variables such as the economic context or market fluctuations. BBVA is not responsible for updating these contents or for giving notice of such changes.

BBVA accepts no liability for any loss, direct or indirect, that may result from the use of this document or its contents.

This document and its contents do not constitute an offer, invitation or solicitation to purchase, divest or enter into any interest in financial assets or instruments. Neither shall this document nor its contents form the basis of any contract, commitment or decision of any kind.

In regard to investment in financial assets related to economic variables this document may cover, readers should be aware that under no circumstances should they base their investment decisions in the information contained in this document. Those persons or entities offering investment products to these potential investors are legally required to provide the information needed for them to take an appropriate investment decision.

This report has been produced by the Digital Regulation Unit:

Chief Economist for Digital Regulation Unit
Álvaro Martín
alvaro.martin@bbva.com

María Álvarez
Maria.alvarez.caro@bbva.com

Vanesa Casadas
vanesa.casadas@bbva.com

Alicia Sánchez
alicia.sanchezs@bbva.com

Javier Sebastián
jsebastian@bbva.com

Ana Isabel Segovia
Ana.segovia@bbva.com

Pablo Urbiola
pablo.urbiola@bbva.com

Javier Anatole Pallás Gozálvez
javieranatole.pallas@bbva.com

With the contribution of:

Arturo Fraile
arturo.fraile@bbva.com

Álvaro Romero
Alvaro.romero.mateu@bbva.com

BBVA Research

Group Chief Economist
Jorge Sicilia Serrano

Macroeconomic Analysis
Rafael Doménech
r.domenech@bbva.com

Global Macroeconomic Scenarios
Miguel Jiménez
mjimenezg@bbva.com

Global Financial Markets
Sonsoles Castillo
s.castillo@bbva.com

Global Modelling & Long Term Analysis
Julián Cubero
juan.cubero@bbva.com

Innovation & Processes
Oscar de las Peñas
oscar.delaspenas@bbva.com

Financial Systems & Regulation
Santiago Fernández de Lis
sfernandezdelis@bbva.com

Countries Coordination
Olga Cerqueira
olga.gouveia@bbva.com

Digital Regulation
Álvaro Martín
alvaro.martin@bbva.com

Regulation
María Abascal
maria.abascal@bbva.com

Financial Systems
Ana Rubio
arubiog@bbva.com

Financial Inclusion
David Tuesta
david.tuesta@bbva.com

Spain & Portugal
Miguel Cardoso
miguel.cardoso@bbva.com

United States of America
Nathaniel Karp
Nathaniel.Karp@bbva.com

Mexico
Carlos Serrano
carlos.serranoh@bbva.com

Turkey, China & Geopolitics
Álvaro Ortiz
alvaro.ortiz@bbva.com

Turkey
Álvaro Ortiz
alvaro.ortiz@bbva.com

China
Le Xia
le.xia@bbva.com

South America
Juan Manuel Ruiz
juan.ruiz@bbva.com

Argentina
Gloria Sorensen
gsorensen@bbva.com

Chile
Jorge Selaive
jselaive@bbva.com

Colombia
Juana Téllez
juana.tellez@bbva.com

Peru
Hugo Perea
hperea@bbva.com

Venezuela
Julio Pineda
juliocesar.pineda@bbva.com

CONTACT DETAILS: BBVA Research: Azul Street, 4. La Vela Building - 4 and 5 floor. 28050 Madrid (Spain). Tel.:+34 91 374 60 00 y +34 91 537 70 00 / Fax:+34 91 374 30 25 - bbvaresearch@bbva.com www.bbvaresearch.com