GENERAL DATA PROTECTION REGULATION, RIGHT TO BE FORGOTTEN, BLOCKCHAIN TECHNOLOGY AND HUMAN RIGHTS

OSCAR CELADOR ANGÓN[1]

Abstract: The aim of this paper is to offer some reflections on the role that new technologies can play in the field of human rights, and specially from the point of view of the general data protection regulation and blockchain technology. The European Union General Data Protection Regulation of 2016 has modified the regulatory framework in key aspects for human rights, such as the consent of the individuals affected by the processing of their data, the right to data portability, or the right to be forgotten.
In line with this approach, the first part of the study focuses especially on the regulation of the right to be forgotten and the rights to privacy and respect for privacy. In the second part of my study, the paper analyses the role that blockchain technology can play in guaranteeing and protecting human rights, as well as in the implementation of the Sustainable Development Goals.

Keywords: General Data Protection Regulation, Right to be forgotten, Blockchain technology, Sustainable development goals, Human Rights.

Summary: 1. Introduction. 2. The General Data Protection Regulation. 3. Right to erasure (right to be forgotten). 3. 1. Court of Justice of the European Union case law. 3. 1. 1. Search engine responsibilities. 3. 1. 2. Requirements for removing links to websites containing personal data. 3. 1. 3. Geographical scope of link removal. 3. 1. 4. Image search results. 3. 2. European Court of Human Rights case law. 4. Blockchain technology and anonymity. 4. 1. Blockchain, GDPR and right to erasure. 4. 2. Blockchain and sustainable development goals. 4. 3. Blockchain and Human Rights 5. Conclusions.

1. Introduction

Law is defined as a tool at the service of society, either to facilitate its transformation or to satisfy its needs. Technology plays a similar role to law, but the difference is that law is a reflection of the wishes of the majority of society, whose representatives make the laws, while technology is created by operators who play by the rules of the market.

The tension between technological evolution and the guarantee of human rights has been constant in the history of humanity. Technological advances have improved the quality of life of human beings in many areas, but their use in certain contexts, such as warfare, has led to the death of millions of people in cruel wars. In other words, while technological evolution is indispensable for eradicating hunger or poverty, it has also allowed human rights violations to become increasingly effective and harmful. The origin of the problem is not in the technology itself, but in the use that human beings make of it.

[1] Universidad Carlos III de Madrid (Oscar.celador@uc3m.es).

Technology can affect the exercise and guarantee of human rights, depending on how it is used. The Internet is probably the best example of how technology can enhance the exercise of human rights, and at the same time seriously harm them. The democratisation of Internet access allows ideological pluralism to be present in digital society, which has positive consequences for the exercise of human rights. However, the exercise of freedom of expression and press may affect the rights to honour, image or privacy, or may have a negative impact on national security, public safety or the rights and freedoms of others.

The aim of this paper is to offer some reflections on the role that new technologies can play in the field of human rights, and we will pay special attention to the general data protection regulation and blockchain technology (BCT). European Union General Data Protection Regulation[2] has replaced the previous Data Protection Directive of 1995, and has modified the regulatory framework in key aspects for human rights, such as the consent of the individuals affected by the processing of their data, the right to data portability, or the right to be forgotten. In this part of our study we will focus especially on the regulation of the right to be forgotten, as the exercise of this right is very relevant from a human rights perspective, given that it has consequences for numerous rights, including the freedoms of expression and information, and the rights to privacy and respect for intimacy.

In the second part of our study, we will analyse the role that BCT can play in guaranteeing and protecting human rights. BTC can play an important role in this context, as it is a technology that theoretically offers a high level of security and protects personal data. BTC has the advantage of guaranteeing the anonymity of personal data, as authenticity is not verified by a third party but by a computer network, but at the same time this technology can facilitate the commission of crimes, due to the anonymity of the operators and the difficulty of tracing their transactions.

Therefore, and always from the perspective of the European Union Data protection regulation, we will first explain how the right to be forgotten is protected, as well as the role played by the Court of Justice of the European Union and the European Court of Human Rights in such protection. And secondly, we will study the role of the BCT in the protection of human rights, and therefore its potential impact on the right to be forgotten, since the main characteristic of this technology is that its data chain cannot be altered to ensure their security and reliability in data transactions, so that the right to be forgotten cannot be exercised when this technology is present. This will allow us to offer some final reflections on the role that the BTC can play in guaranteeing and protecting human rights.

2. The General Data Protection Regulation

The European Union General Data Protection Regulation (GDPR) was adopted on 14 April 2016 and became enforceable on 25 May 2018, replacing Directive 95/46/EC.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). ELI: http://data.europa.eu/eli/reg/2016/679/oj (access 22/2/2024).

The main purpose of the GDPR is to protect natural persons with regard to the processing of their personal data and the free movement of such data.

GDPR has to be interpreted according with the Charter of Fundamental Rights of the European Union, article 8 of which provides that: "Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the data subject or on another legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority". However, data protection is not an unlimited right, as Article 52 of the Charter states that the rights protected in the Charter may be limited by law, provided that their essential content is respected, and when the limitations are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others (Consejo Económico y Social, 2017)

In the following lines, I will refer briefly and in a non-exhaustive manner to the main new features of the GDPR, insofar as they may affect the exercise of human rights.

Firstly, one of the main new features of the GDPR is that compliance does not refer to European countries, but to those that offer goods and services in the European Union regardless of whether they are European. Individuals and companies operating in the European Union will be responsible for the processing of personal data, will have to comply with a number of rules related to the security of data processing and the appointment of a data protection officer, and may be subject to very serious sanctions in the event of data protection breaches. GDPR is very clear in stating that "this Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not (Art. 3).

In consequence, GDPR standardised member states' regulations, because Directive 95/46/EC allowed states to adopt a regulatory framework that was sometimes different, since it granted a high margin of appreciation to the states. The main consequence of previous regulation was that many non-European companies established themselves in those countries with lighter legislation in the field of personal data processing and marketing (Sancho López, 2018).

GDPR has organised data traffic between the European Union and the United States, given that US regulations are lighter and European protection standards are higher, so that, regardless of their nationality, all companies that operate in the European Union and wish to interact with European citizens must comply with European regulations (Fernández, 2016). In case of personal data protection conflicts, the previous regulation forced the parties in many cases to litigate in US courts, since the large international companies that trade with personal data had their headquarters there, as US regulation is very permissive in this area (Sancho López, 2018, p. 17).

Secondly, in order to improve users trust, data should be processed in a way that ensures adequate security and confidentiality of personal data, for which data processors may be required to establish certification mechanisms and data protection seals and marks (GDPR Art. 42, Recitals 39 and 100).

Thirdly, the rules on consent have been amended, so that for consent to be valid a number of requirements must be met, and "the controller must be able to demonstrate that the data subject has consented to the processing of his or her personal data [...] the request for consent shall be presented in a way that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language" (GDPR, art. 7.1, 2). The data controller can only process data when the data subject consents to the processing of his or her data freely, having received all the information regarding both the processing of his or her data and the consequences of consenting to the processing. Finally, the data controller must also be able to prove that the data subject consented to the processing of his or her data. (Cardó, 2018).

The data subject has the right to withdraw or modify his or her consent at any time during the processing of his or her data, for which an accessible and simple procedure for consent or withdrawal of consent must be available (Álvarez, 2018).

To this end, GDPR requires data processors to seek the specific, informed, unambiguous and explicit consent of their users. The basic requirements for the effectiveness of a valid legal consent are defined in Article 7 and specified further in recital 32 of the GDPR. In concrete: "consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an Internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided".

In this context, it is important to note that, in accordance with Article 6 of the GDPR, consent to the processing of your personal data for one or more specified purposes, although particularly relevant, is for practical purposes only one of the six cases in which data processing is lawful. Likewise, "consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. When asking for consent, a controller has the duty to assess whether it will meet all the requirements to obtain valid consent. If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful" (European Data Protection Board, 2020, p. 5).

Fourthly, GDPR protects the right to portability, so individuals can ask companies to provide them all the personal data they have in storage (GDPR, article 14. 2. C). The Right to data portability is defined as the right of the data subject, on the one hand, to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided; and on the other hand, as the right to have the personal data transmitted directly from one controller to another, where technically feasible (GDPR, article 20.1, 2). The right to data portability is not unlimited, and must be exercised in compliance with the tasks carried out in the public interest or in the exercise of public powers vested in the controller, and in any case may not adversely affect the rights and freedoms of third parties.

Finally, article 17 GDPR expressly recognises the right to be forgotten. Prior to the adoption of the GDPR, the Court of Justice of the European Union interpreted Directive 95/46/EC in such a way as to guarantee the right to be forgotten (Mieres, 2014). This is a very relevant right from a human rights perspective, as it affects, among others, the rights to freedom of expression, information, privacy and image. The GDPR opts for an open formulation of the right to be forgotten, due to the difficulty of offering closed solutions in a context in which it is necessary to analyse the circumstances of each specific case.

3. Right to erasure (right to be forgotten)

The global nature of the Internet and social networks generates a multiplier effect, regardless of the intentions of their operators, which can have very negative consequences on the image of individuals, as well as in their right to privacy. The Directive 95/46/EC was adopted at a historical moment when the internet was in its infancy, hence the law did not adequately regulate certain matters related to the expansion of the internet, such as the protection of personal data on the web, the use of search engines, or the use of the Internet and the protection of privacy (Guichot, 2019).

The recognition of the right to be forgotten in the GDPR, regarless of the fact that this right had already been recognised by the Court of Justice of the European Union in its interpretation of Directive 95/46/EC, is a clear message to search engines and data controllers. The exercise of the right to be forgotten depends on which data subject has requested deletion, as well as on whether the data they want to delete are (or are not) necessary for the purposes for which they were collected (Fernández, 2016, p. 400).

GDPR guarantees the right to be forgotten as an autonomous right, according to the following formula: "1.The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)" (Article 17.1).

As Guichot has pointed out, "it is a regulation that encompasses the "old" right of cancellation and the "new" right to be forgotten, with the peculiarity in the latter that universal access to the personal data of third parties is possible because they are published on the web, and on which the precept seems to point to the obligation of publishers to prevent indexing in these cases through the corresponding technical measures" (Guichot, 2019, p. 80). In the words of Zárate, "it is a right to cancel personal data, which confirms that the title "right to be forgotten" is in reality a right consisting of the claim to forget or be forgotten, so that the "right to be forgotten" should not be considered as anything more than a fancy term to qualify a right to cancellation, rectification or opposition" (Zárate, 2013, p. 3).

The right to be forgotten may be refused in certain cases, and in particular: to guarantee the right to freedom of expression and information; for compliance with a legal obligation requiring processing under European Union or Member State law to which the controller is subject; in certain situations, to protect the public interest in the area of public health; for archival purposes in contexts of public interest, or for scientific or historical research purposes or for statistical purposes; and finally for the establishment, exercise or defence of legal claims (Article 17. 3). The above-mentioned cases are very generic, and aim to protect the public interest in certain contexts (health, judicial, scientific or historical research), as well as certain fundamental rights, such as the freedoms of expression and information, the content of which would be emptied if the right to be forgotten were unlimited. The formulation of the right to be forgotten is very generic, due to the relevance of the rights involved in this context, which gives the courts a high role in determining the content of this right (Soriano, 2018).

I will now refer to the decisions of the Court of Justice of the European Union and the European Court of Human Rights, in order to understand the content of the right to be forgotten, especially when this right conflicts with the right to access information, or to protect the public interest in the above contexts. In this regard, it is important to bear in mind that we do not intend to analyse all the decisions of the courts referred to, as this would go beyond the scope of this paper, but only to explain their main decisions related to the right to be forgotten.

3. 1. Court of Justice of the European Union case law

3. 1. 1. Search engine responsibilities

Prior to the adoption of GDPR, The Court of Justice of the European Union (CJEU) has ruled on this issue in Google Spain, S.L. and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González[3]. This is a landmark court decision, which was adopted in the context of Directive 95/46, in which the court defined for the first time the role of search engines in relation to the right to be forgotten (Article 29 data protection Working Party, 2014) (Torres Manrique, 2018) (Aguinaga, 2022) (Buisán, 2014) (Boix, 2015).

Mr Costeja González complaint against a Spanish newspaper (La Vanguardia), and against Google Spain and Google Inc. The complaint was based on the fact that, when an Internet user entered Mr Costeja González's name in the search engine of the Google group, he would obtain links to two pages of La Vanguardia's newspaper, on which an announcement mentioning Mr Costeja González's name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts.

As regards the activity of search engines as providers of content in relation to Directive 95/46, the Spanish "Audiencia Nacional" asked the Court of Justice the following question: "in relation to the activity of [Google Search], as a provider of content, consisting in locating information published or included on the net by third parties, indexing it automatically, storing it temporarily and finally making it available to Internet users according to a particular order of preference, when that information contains personal data of third parties: must an activity like the one described be interpreted as falling within the concept of "processing of … data" used in Article 2(b) of Directive 95/46?" In addition, the court had to establish whether the processing of data by search engines is subject to EU data protection rules, as well as whether individuals have the right to request that links to their personal data do not appear in the results of an Internet search carried out under their name.

With regard to the definitions of "processing of personal data" and "controller", provided by Article 2(b) and (d) of Directive 95/46/EC, the Court stated that "first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of Article 2(d)" (paragraph 100).

[3] ECLI identifier: ECLI:EU:C:2014:317

The court differentiated between the role of the search engine and that of the website on which the information is hosted. According to the court, the operator of the search engine has to remove the information from the list of results -obtained after a search on the basis of a person's name links to web pages- published by third parties and containing information relating to that person, regardless of whether the website on which the information is hosted does not delete the information, and regardless of whether the publication on the website is lawful or unlawful.

Regarding the processing of personal, as Recio has pointed out, "it is not until the user carries out the search, using the name of the person as criteria, that the processing of personal data takes place, without the search manager again determining the purposes of the processing, since it provides a tool, the search engine, which will be used by the user to search for content on the basis of the search parameters that he decides. And in that decision, relating to the use of the search engine and the search parameters, the search engine does not participate, so it must be excluded from the concept of data controller because it does not determine one of the essential elements that are key to considering it as such" (Recio, 2020, p. 88).

Article 9 of Directive 95/46 established that member States shall provide for exemptions or for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression. The only exception in this context would be where the person concerned is a public person, so that the interference would be justified precisely by the public's interest in accessing the information. In consequence, the court made a balance between the right to access information and the right of individuals not to be able to find personal information, and established that the right of the individual to request that his or her personal information not be made available to the general public by inclusion in a list of search results overrides, on the one hand, the economic interest of the search engine operator and, on the other hand, the public's interest in accessing the information in a search on that person's name.

Therefore, European citizens have the right to request search engines to remove information related to their personal data, and if the complaint is well-founded the search engine operator must comply with the request. However, while the court made it clear that search engines must remove certain information from the list of results in specific cases, the media (in this case the Spanish newspaper) is not obliged to remove the information it offers to the public.

According to the court's construction, the right to be forgotten means that users have the right to have search engines not display some of their results, when these may be qualified as "inadequate, irrelevant or no longer relevant, or excessive". The right to be forgotten, while allowing information to be removed or hidden from search engines, does not include the right to have personal data deleted from a website. Consequently, information that may affect the privacy or image of individuals will still be accessible to the public, but it will be more difficult to access as it will not be accessible by search engines.

The right to be forgotten collides with the right to access information, so the court limits the exercise of the right to be forgotten in the case of information relevant to the public interest or concerning politicians or public figures. This position has raised a few questions connected to the definition of the term "public interest", such as when information ceases to be of public interest, what parameters search engine operators should use to decide when to remove or modify search results, or what the public's interest in accessing information is.

The right to be forgotten can be exercised autonomously, either against the original source of information or against the search engine. In the event that search engines do not accept the request, it is possible to appeal to the national agency responsible (in the case of Spain, the "national data protection agency"); and finally, the decision of the national agency can be appealed before the courts.

3. 1. 2. Requirements for removing links to websites containing personal data

In GC and Others v Commission nationale de l'informatique et des libertés[4], the plaintiffs requested Google to remove various links to web pages published by third parties from the list of results obtained by the search engine operated by Google, following a search carried out on the basis of their names. Google refused to remove those links, and the plaintiffs therefore appealed to courts. The French Conseil d'État refered several questions to the Court of Justice for a preliminary ruling. Among the questions asked, the following are particularly interesting: does the prohibition imposed on the operator of a search engine from processing personal data, oblige it systematically to accept requests for removal relating to links leading to websites which process such data?; where the links the deletion of which is requested lead to the processing of personal data solely for journalistic purposes or for the purposes of artistic or literary expression, may the operator of a search engine refuse to accept that request?; and if the applicant proves that such data is incomplete, inaccurate or out of date, is the operator of a search engine obliged to accept the corresponding withdrawal request?

The activity of search engines and Internet publishers is technically different, as publishers make information available to third parties on a website, while search engines facilitate access to websites by enhancing communication and the transfer of information to their customers. The court noted that search engine operators are subject to Directive 95/46, as they process personal data and the operator is the data controller. The activity of search engines has direct consequences on the fundamental rights to respect for private life and the protection of personal data, and their activity must therefore respect the limits and guarantees indicated in Directive 95/46.

Article 8(1) and (5) of Directive 95/46 prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life. However, it removes this prohibition in the following

[4] ECLI identifier: C:2019:773

cases: if the data subject has given his or her explicit consent to such processing; the processing is necessary in order to comply with the specific employment law obligations and rights of the controller; the processing is necessary in order to safeguard the vital interests of the data subject or of another natural or legal person who is incapable of giving his or her consent; processing is carried out in the course of its legitimate activities and with appropriate safeguards by a foundation, an association or any other non-profit-making body whose purpose is political, philosophical, religious or trade union, provided that it relates exclusively to its members; processing relates to data which the data subject has manifestly made public or is necessary for the establishment, exercise or defence of a right in legal proceedings; and processing of data relating to offences, criminal convictions or security measures.

The court ruled that when search engine operators are required to remove links to websites where the personal data concerned are published, they must, on a case-by-case basis, examine whether the inclusion of such a link in the list of results obtained after a search based on the name of the data subject is strictly necessary to protect the freedom of information of Internet users. With regard to information relating to legal proceedings, the court noted that search engines must remove links to websites that provide information from "an earlier stage of the legal proceedings in question and, in view of the development of those proceedings, are no longer relevant to the current situation" (para. 80). In such cases, search engine operators must strike a balance between the right to privacy of the searched person and the right of Internet users to obtain information.

3. 1. 3. Geographical scope of link removal

In Google LLC v Commission nationale de l'informatique et des libertés[5], the court ruled on the geographic scope of search engine link removal ordered under Directive 95/46. Google's position was to apply the right to be forgotten exclusively to its French search engine, given that the claim was brought by the French data protection authority. However, the court established that the right to be forgotten, although given the court's jurisdiction it could not be interpreted worldwide, was enforceable at EU level.

In the court's opinion, "when a search engine operator grants a request for de-referencing pursuant to those provisions, that operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an Internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request" (paragraph 74). Additionally, search engine operators must prevent an Internet user searching from one member state, on the basis of a data subject's name, from accessing links or search results that have been

[5] ECLI identifier: EU:C:2019:772

altered in another EU country in order to guarantee the right to be forgotten (Samonte, 2019) (Pirkova, Masséeu, 2019).

According to the court, the right to be forgotten is limited to the activity of search engines, as the information that is considered harmful continues to be hosted on the web server, although its visibility is significantly limited even though it may be legitimate information protected by the rights to freedom of expression and information. The right to be forgotten only applies to search engines with domain names associated with EU Member States, e.g. google.fr as well as google.es or google.it, but is not enforceable for all other versions of a search engine worldwide. as many non-European countries do not recognise the right to be forgotten. And finally, it is important to bear in mind that search engines can offer information that is removed from their search results in the European Union outside their territory, as this is a context in which the Court has no jurisdiction.

3. 1. 4. Image search results

The judgment of the Court of Justice of 8 December 2022 in TU, RE v Google LLC[6] illustrates the Court's position regarding image search results. The Court had to make a balance between the rights protected in Articles 7 and 8 (the rights to Respect for private and family and to Protection of person) and those protected in Article 11 (the Freedom of expression and information) of the Charter of Fundamental Rights of the European Union. The plaintiffs had managerial responsibilities in investment firms, and requested Google to remove the search results for their names from the search engine, as they claimed they included links to three articles highly critical of their firms' business model, with images suggesting that they led a life of luxury, and containing inaccurate allegations and defamatory opinions. In addition, the plaintiffs requested the removal of photos of them in the form of thumbnails from the list of results of an image search based on their names. Google denied the request, as in their view they were detrimental to their image.

Search engines do not need consent to provide information, as it would be impossible to obtain such consent a priori for all results, so the process of removing information from search engine results requires those concerned to tell the search engine what information they do not consent to appear in their results. However, the most complex part of the exercise of the right to be forgotten, as Pirkova and Massé have pointed out, occurs when "a search engine still has to balance the data subject's fundamental rights and the public's right to freedom of information, taking into consideration complex criteria such as the nature and seriousness of the offence in question, the progress and the outcome of the proceedings, the data subject's role in public life, and the level of public interest in the information at the time of the removal request" (Pirkova, Massé, 2019).

The Court reached three conclusions. First, search engine operators must ensure that the safeguards established by Directive 95/46, with the aim of protecting the fundamental

[6] Case C-460/20, ECLI:EU:C:2022:962

rights to respect for private life and to the protection of personal data, are effective. Second, when search engine operators receive requests to remove links from their results, they must check the extent to which the right of Internet users to access information is affected. And third, the GDPR requires that in case of conflict, a balancing of the rights to respect for privacy and personal data protection against freedom of information must be carried out. This requires a case-by-case assessment of: the nature of the information concerned, the sensitivity of the dissemination of the information to the privacy of the data subject, and the public interest in having the information.

The court ruled that image search results, regardless of whether they are in the form of previews, may constitute an interference with the rights to protection of privacy and personal data, and that "by retrieving the photographs of natural persons published on the Internet and displaying them separately, in the results of an image search, in the form of thumbnails, the operator of a search engine offers a service in which it carries out autonomous processing of personal data which is distinct both from that of the publisher of the Internet page from which the photographs are taken and from that, for which the operator is also responsible, of referencing that page" (paragraph 103). In other words, the presentation of images in the form of previews may entail an additional interference with the rights to respect for privacy and to the protection of personal data, since it allows Internet users to access information that is complementary and autonomous to the main information.

In order to know what is the informative value of photographs, the court pointed out that it is necessary to differentiate between those that are displayed as a preview in a search engine's list of results, and therefore out of the context in which they were published on the original web page, and those photographs that are part of the information as they illustrate the article and the opinions expressed therein.

Therefore, the court has resolved disputes related to image search results using the same criteria as in cases related to the removal of links to websites containing personal data, interpreting that images are part of personal data, and that images do not need specific or different protection from personal data.

3. 2. European Court of Human Rights case law

Technological progress has allowed the Internet and social networks to become huge repositories of information, which can be stored for unlimited time. The storage function can have positive implications for human rights, but it also amplifies the networks' ability to affect people's image and privacy.

GDPR establishes that freedoms of expression and information can limit the right to be forgotten. These rights are connected to the freedom to communicate beliefs, ideas and opinions. The balance between these rights is very important, as unrestricted exercise of the freedoms of expression and information would convert the right to privacy meaningless. But an unrestricted right to privacy would be equivalent to censorship of the freedoms of expression and information. Access to information is fundamental in the framework of a democratic and pluralistic society, as access to information is essential for the formation of public opinion. The freedoms of expression and information are complemented by the right to obtain ideas or opinions, but these must respect public order, constitutional principles and the rights and freedoms of others.

The European Convention on Human Rights (ECHR) offers some clues in this respect, when it sets out the limits to freedom of expression and the content of the right to privacy. The ECHR does not explicitly protect the right to data protection, due to the date of its adoption, but its article 8 protects the right to respect for his private and family life, but this right may be limited in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. Article 10 of the ECHR states that freedom of expression shall include freedom to hold opinions and to receive and impart information and ideas. States may restrict freedom of expression in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the reputation or rights of others.

Before entering into the study of the decisions of the European Court of Human Rights, it is important to note that, due to the large number of decisions of the Court on the freedoms under Article 10 ECHR when they collide with the rights protected by Article 8 ECHR, we will limit our analysis to two of its decisions, in order to describe in a comprehensive way what the Court's position is in this context.

In the case of M.L. and W.W. v Germany[7] the European Court of Human Rights (ECtHR) ruled about a German Federal Court of Justice decision, prohibiting three different media from continuing to allow Internet users access to documentation concerning the applicants' conviction for the murder of a famous actor and mentioning their names in full. The plaintiffs requested both that the information with their names be removed from search engines as this facilitated access to the information by Internet users, and that the media publish and retain the information with their names on their websites. As a starting point, the court noted the importance of the press in democratic opinion-forming by making available to the public old news that had been kept in its archives.

The court ruled in favour of freedom of information, agreeing with the German Federal Court of Justice. In this particular case, the court had to decide between the public's right to be informed about past events and the right to anonymity of a person who had been the subject of an Internet publication. The court recalled its doctrine, which has repeatedly established that the way in which news is treated, as well as the information it contains, must be decided by journalists in accordance with their profession's ethical and deontological regulations.

[7] Application nos. 60798/10 and 65599/10, 2018

In this particular case, the inclusion of individualised information about the protagonists of the news was relevant, as it was related to a criminal trial with a high impact in the media. This information contributed to forming public opinion, and the public had the right to know the details of the news, especially the conduct of their criminal trial and their requests for the reopening of that trial. In fact, the applicants had contacted the media when they requested to reopen the criminal proceedings, so that their right to anonymity had thus been very limited.

Finally, the news for which amendment was sought only described the proceedings and the court decision in a factual manner, and could not be described as denigrating or damaging to the plaintiffs' reputation. The court therefore held that the plaintiffs' right to privacy had not been infringed.

The European Court of Human Rights has ruled in the case of Hurbain v Belgium[8] that a rehabilitated offender has a right to be forgotten. A civil judgment ordered the publisher of the Belgian daily newspaper "Le Soir" to anonymise the archived electronic version of an article mentioning the full name of G., the driver responsible for a fatal road accident in 1994, on the basis of the right to be forgotten.

The court ruled from the perspective of the right to be forgotten under Article 17 of the GDPR, and in particular on the right to obtain from the controller the erasure of personal data that are no longer necessary for the purposes for which they were collected or otherwise processed, as well as the connection of the information concerned with the exercise of the right to freedom of expression and information. The judicial debate did not focus on the lawfulness of the article when it was first published, but on the fact that it was available on the Internet and on the possibility of accessing the article long after the events.

The court ruled in favour of the right to be forgotten, and established that: "the domestic courts weighed in the balance G.'s right to respect for his private life and the applicant's right to freedom of expression, in accordance with the criteria established in its case-law. Specifically, the Court of Appeal attached particular weight to the damage sustained by G. on account of the online publication of the article in question, having regard in particular to the passage of time since the publication of the original article and to the fact that the anonymisation of the article on the website of Le Soir left the archives themselves intact and constituted the most effective measure amongst those that could have been taken in the present case, without interfering disproportionately with the applicant's freedom of expression. In the Court's view, the reasons given by the domestic courts were relevant and sufficient […] The Court wishes to make it clear that its finding cannot be interpreted as entailing an obligation for the media to check their archives on a systematic and permanent basis. Without prejudice to their duty to respect private life at the time of the initial publication of an article, when it comes to archiving the article they

[8] Application no. 57292/16, 2021

are required to carry out a check, and thus weigh the rights at stake, only if they receive an express request to that effect" (paragraphs 132, 135).

The solution proposed by the Belgian courts was to anonymise the article published on Le Soir's website by replacing G.'s first name and surname with the letter X. With this formula, it was not necessary to remove the article from the newspaper's archives, only to anonymise the electronic version, and this solution allows the newspaper to guarantee the integrity of the original digital version. From this perspective, the interference with the newspaper's right to freedom of expression was minimal and proportional to the exercise of the right to be forgotten.

The European Court has resolved the conflicts between the freedoms of expression and information and the right to be forgotten, on the one hand, by differentiating between the role of search engines and the media; on the other hand, by taking into account the peculiarities of each case, and trying not to sacrifice any of the rights at stake unless there is no other possibility; and finally, the court is not in favour of modifying digital files with personal data, when they do not unjustifiably affect the image and reputation of individuals, as this would mean censoring freedom of information and access to information.

4. Blockchain technology and anonymity

Blockchain is based on a chain that chronologically orders a series of transactions that are recorded identically in a computer network. The blocks that make up the chain are connected, each block incorporates the information of the previous block, in accordance with a protection system that prevents the deletion or alteration of the data chain. Therefore, users participating in the blockchain add their information creating an irreversible chain (G'sell, Martin-Bariteau, 2022, p. 6). As Mhlanga has noted, "blockchains are a type of digital ledger that cannot be altered without leaving clear evidence of having been altered. Since these digital ledgers are deployed in a distributed fashion, there is typically no central repository or authority, such as a bank, corporation, or government. This is due to the lack of a necessity for a centralized repository and authority" (Mhlanga, 2023, p. 2). The philosophy of BCT is that stored information is protected by a peer-to-peer network, which eliminates the risks of centralised databases.

The transactions with BCT are carried out between computers or nodes in peer to peer mode, the user's public profile is validated through a series of algorithms, and once the validation is completed, a new block is created and added to the existing ones, creating an unalterable and permanent chain that can only be modified through new transactions. Blockchain was initially designed to bring security to commercial and financial transactions, especially in the field of cryptocurrencies due to the reliability of this technology and the high level of security it offers, given that it does not use a central server or third parties to verify transactions, as these are encrypted and replicated on all the computers of the network users (Bartolomé, Lindín, 2018).

The main characteristics of the blockchain are: technological security, autonomy of the system, and transparency and anonymity of the operators.

The system is secure, as the information is not stored physically or digitally in a file, but is stored in computers that verify their relationships using complex algorithms. Unlike other systems, blockchain does not use a central authority to manage the information stored in the blockchain, which prevents unwanted third parties or hackers from accessing the information. Each blockchain is a unique and independent unit that theoretically cannot be intervened by third parties, making it one of the most secure technologies currently available. This ensures confidence in the process and in the transactions. (Bilbao, 2019, p. 4).

From the perspective of the right to be forgotten, how can personal data be removed from a blockchain network when a person revokes their consent? The answer to this question is complex, as blockchain technology means that all nodes participating in the blockchain can access all data stored in the chain, so that all parties have the same copy of each transaction. This is the strength of this technology.

The blockchain system is autonomous, as the verification processes of the public and private codes of the operators are carried out outside the operators, so that a node reads the information and incorporates it into the blockchain. This model eliminates intermediaries between the parties, through an autonomous and independent model that guarantees anonymity and trust in the blockchain system (Weinstein, 2016).

And finally, BCT is characterised by the transparency and pseudo-anonymity of the operators. Each node has a complete copy of the information chain, so that any operator can access the information and know all the transactions that take place in this context. Transparency is complemented by the anonymity of the operators, as users can participate and operate on the network without providing personal data. Individuals operate using two codes, one public and one private. The public code identifies the person and is known to the rest of the operators, and may not contain any personal data or data related to the operator’s identity; while the private code is known only to each operator and serves to validate operations, signing and/or authorising them. Behind the public address of an operator can be an individual, an NGO or a company, thus allowing the operation to be anonymous for all intents and purposes. The same operator can have multiple public codes, and the creation of these codes does not require the use of the operator’s personal information, which guarantees anonymity.

4. 1. Blockchain, GDPR and right to erasure

GDPR encourages the movement of data within the European Union according to two principles. Firstly, natural or legal person operating in the European Union are responsible for the processing of personal data, so there must be a data controller in charge of guaranteeing users’ rights in the processes. GDPR provides that data controller means: “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law” (Article 4). And secondly, users may exercise the right to be forgotten in accordance with certain requirements.

These principles may be incompatible with blockchain, because this technology is characterised by the anonymity of the operators and the transparency of the process. In other words, the absence of third parties in BCT, which a priori is one of its virtues, may be a drawback in the context of the GDPR. Likewise, the GDPR sometimes requires the modification or deletion of data to allow the exercise of the right to be forgotten, which is not possible in the case of BCT, as it is precisely the difficulty of altering the blockchain that is the key to its security and reliability in data transactions.

As pointed out by G'sell and Martin-Bariteau, "Two key features of BCT seem to be particularly problematic: the transparency and immutability associated with blockchains. As mentioned above, many blockchain platforms are designed with transparency in mind, so that transactions can be seen by anyone and those making them are eventually identifiable. This presents risks for users and potential liability for platform operators. Moreover, the principle of immutability that guarantees the integrity of the blockchain and avoids contradictions runs counter to the rights of accuracy and suppression. In principle, any attempt by a user to delete or overwrite existing data will be detected by others and corrected" (G'sell, Martin-Bariteau, 2022, p. 33). In the words of Mendoza, "despite the obvious benefits, there are some obstacles to compliance with the regulations on the protection of personal data in the blockchain service, linked to the exercise of the so-called ARCO rights, specifically to the rights of rectification and cancellation of personal data, as well as the determination of the figure of Responsible for data processing" (Mendoza, 2020, p. 109).

GDPR defines a data controller as follows: "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law" (article 4, paragraph 7). In the case of blockchain, it is very difficult to know who the data controller is, especially since blockchain uses a peer-to-peer (P2P) network made up of a set of computers that behave as equals to each other.

Private companies managing blockchain have the responsibility that GDPR attributes to data controllers. In the case of public companies, according to Mena, blockchain users would be co-responsible because they have decided to use the BCT, although they cannot modify the information chain, not even when they are responsible for it, but it is not clear who is the data controller for the purposes of the GDPR (Mena, 2021).

Personal data is defined in GDPR as: "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" (Art. 4, paragraph 1). The definition refers to "any information", so the term "personal data" should be interpreted as broadly as possible. Data that are part of the blockchain are personal data, even if they are not associated with a person, when such data allow the person to be identified by any means, such as, for example, the IP address (Castello, 2021). BCT uses data that is considered personal data, both in terms of the public and private code that guarantees access to the information. Data on the blockchain is encrypted using a verification system that allows the information to be de-encrypted and accessed.

The key question is: how can the right to be forgotten be harmonised with the impossibility to modify the blockchain data chain? The main virtue of the blockchain is that its registry is decentralised, so that there are numerous copies (which cannot be modified) with all the information, in order to guarantee the security of transactions.

Among the technical solutions that can be adopted for BCT to comply with GDPR, it has been proposed not to record personal or private information in the blockchain, but in an autonomous database, so that only the URL and the cryptographic hash value of the personal information into the blockchain would be recorded in the blockchain (Tanaka, Hiroyuki, 2019). With this measure, the rights to rectification and to be forgotten could be exercised, as the information in the external database is alterable but not shared and could be encrypted to protect the information. Likewise, the information contained in the blockchain would have no personal or personally identifiable information. Another solution proposed in this context has been to hide the block from search results in search engines, so that although the information is still present, it cannot be displayed (Castello, 2021).

The right of erasure guaranteed by the GDPR can also be exercised through "irreversible anonymisation processes", which make the data to be erased inaccessible. In the case of personal data, the creation of new records containing the updated information and, consequently, the personal data already rectified has been proposed through the erasure of the previous records containing the information to be rectified (Mendoza, 2020, p. 116). Another solution proposed to resolve the conflict between the possibility of deleting personal data and the BCT is the use of IoT devices. (Grigera del Campillo, 2021).

It is therefore necessary for BCT to adapt to the GDPR regulation, allowing data to be deleted or modified (guaranteeing the rights of rectification and to be forgotten), as well as identifying a data controller who is responsible for data processing. In order to harmonise the immutable nature of blockchain with the GDPR, G'sell, Martin-Bariteau have proposed, on the one hand, to add new transactions to the blockchain, so that blocks are not modified or deleted, but the initial information is effectively supplemented; and on the other hand, when blockchains are encrypted, it is possible to destroy the encryption key, which will prevent access to the data (G'sell, Martin-Bariteau, 2022). In this line, it has been proposed to alter blockchain core elements without denaturing it. A system has been designed in which permissions are granted for a controlling entity to access information (with the ability to identify participants and their activities). This would comply with GDPR but at the cost of losing the full shield on the total anonymity of blockchain users (Reform.uk, 2018).

It is important to note that the EU has shown its interest in BCT through different projects, such as the EU Blockchain Observatory & Forum, which is an initiative of the European Commission to "accelerate blockchain innovation and the development of the blockchain ecosystem within the EU and thus help consolidate Europe's position as a world leader in this transformative new technology"[9]; as well as the European Blockchain Services Infrastructure, which has been designed by the European public sector to be interoperable with private sector platforms.

The European Commission has joined this initiative through the so-called Multi-Country Digital Projects, discussed so far with the Member States in the framework of the Recovery and Resilience Mechanism, which propose "to develop, deploy and operate a Pan-European blockchain-based infrastructure that is green, secure and fully compliant with EU values and legal framework, making the provision of cross-border, national and local public services more efficient and reliable and promoting new business models" (Comisión Europea, 2021, p. 19). The European Commission wants to design sustainable digital infrastructures that are secure and efficient, because it is aware that if the European Union wants to lead the digital revolution it needs a pioneering and sustainable digital infrastructure that allows European industry to be competitive, and currently this option requires the use of BCT.

Justice is also one of the targets of the European technological project, as pointed out by the European Commission in its "Guidelines for the Action Plan", where it stated that both artificial intelligence and BCT could have a positive impact on e-Justice. To this end, it proposes to study the possibilities of blockchain in the context of digital justice, as although "any future development and deployment of this type of technology must take into account the risks and challenges, particularly in relation to data protection and ethics", this technology could have a positive impact on e-justice, increasing the efficiency of the administration of justice and the confidence of European citizens (European Council, 2019, & 30, 31).

A final example can be found in Regulation (EU) 2023/1114 of 31 May 2023 on markets in Crypto-assets adopted by the European Union, which has established an innovation-friendly regulatory framework for EU financial services that does not hinder new technologies, including the use of crypto-assets, which is one of the main applications of BCT in the financial context (Fernández, 2023).

It would not make much sense for the EU to bet on a technology that is not viable within the framework of EU regulation. Therefore, it seems clear that in the medium term EU regulation and BCT have to be compatible, and solutions have to be found that, while guaranteeing the human rights of European citizens, satisfy the interests of all parties involved.

[9] Vid. https://www.eublockchainforum.eu/ (access 22/2/2024).

4. 2. Blockchain and sustainable development goals (SDGs)

The characteristics of blockchain technology, and especially the anonymity of operators, can make it difficult to exercise the right to be forgotten. However, these same characteristics give blockchain technology the capacity to offer trust to consumers, which is why it has many applications in the field of the Sustainable Development Goals (SDGs). (Deshmukh, 2020).

The main inconvenience of this technology for developing countries is that in order to be effective, it is necessary to invest resources in its development and implementation, and this is sometimes not feasible in poorer countries. In addition to this, Blockchain applications are often designed primarily to generate economic benefits for their creators, without taking into account that they can indirectly have a positive impact on developing countries. For this reason, some authors have argued that International human rights organisations, led by the United Nations, should assist developing countries in this context, as it would not make sense to design technological applications focused on SDGs implementation that exclude countries with fewer economic and technological resources. (Mattila, Dwivedi, Gauri, Ahbab, 2022, pp. 237-8).

I will now refer to some examples in order to illustrate the extent to which BCT can help to achieve the SDGs.

The possibility of knowing precisely the origin of the products we consume refers both to the origin of raw materials and to the working conditions under which the producers of services work. In both cases, SDG 8 Decent Work and Economic Growth and SDG 12 Responsible Consumption and Production are protected.

Economic and technological poverty is connected to the difficulty of accessing banking services, which can be alleviated through blockchain technology, although it is necessary to take in account that technological education and basic technological resources are necessary. The United Nations Development Programme (UNDP) is a pioneer in this field[10], as it allows "unbanked" money transfers, using BCT to carry out financial transactions. The only requirements are Internet access, a smartphone and the ability to digitally identify one's identity. This option eliminates the fees of financial intermediaries, and allows banking without having to rely on a banking model that sometimes excludes people without financial resources.

Blockchain can be very useful in combating financial exclusion, as any tool that allows access to the Internet enables individuals to carry out financial transactions through a platform that allows users to operate digitally. In addition, individuals can receive subsidies or income without paying bank fees, and avoid the security problems that are characteristic of the most disadvantaged societies (Mhlanga, 2023, p. 5).

[10] Vid. https://www.undp.org/es (access 22/2/2024).

Cryptocurrencies are very relevant in this context, as many NGOs receive donations in this way, and even some organisations, such as UNICEF, are using cryptocurrencies to make important investments in startups in developing and emerging economies (Deshmukh, 2020). The reliability of the blockchain is seen in its success in gaining user confidence in cryptocurrency transactions, which are almost exclusively carried out using this technology. One example of the application of blockchain to sustainable development goals is the use of Ethereum cryptocurrencies by the World Food Programme to purchase food vouchers for Syrian refugees (Borrero, 2018).

SDG 16 proposes the creation of effective, accountable and inclusive institutions at all levels. BCT can help reduce corruption in public contracts, which are sometimes used by political leaders to enrich themselves, due to the lack of transparency of this type of public contracts. BCT is also very useful for controlling the use to which aid or food resources received by developing countries are used, given that sometimes a large part of this aid is lost in the distribution chain and does not reach its potential recipients. Controlling the destination of funds will not only increase the development aid received by the neediest countries, but will also lead to an increase in donations and donors, who sometimes do not want to cooperate with some needy countries, for fear that corruption will take a large part of the aid, or that it will be used to finance anti-democratic political regimes that do not respect human rights (Deshmukh, 2020).

The transparency and security of BCT make it an important ally in the context of environmental stewardship, where the following possibilities have been identified to maximize the benefits of blockchains: controlling greenhouse gas emissions by optimising carbon markets, decarbonising the electricity sector by increasing the percentage of energy generated by renewable sources or energy, or ensuring sustainable water management, especially due to the increase in demand and the increase in cases of permanent drought (Bilbao, 2019, p. 16). BCT provides relevant information related to the manufacturing chain and logistics, which can affect consumption habits and redirect them towards responsible, sustainable and environmentally friendly choices.

Among the practical applications in the field of SDGs, some authors highlight the following. In some countries (e.g. Thailand), the poor are unidentified, and digital identification has made it possible both to identify the poor and to enroll them in aid programmes. Some countries, such as Cuba, have implemented a medical data programme that, thanks to the security of BCT, allows patients' medical records to be available in most of the country's medical institutions; these applications can also be used to protect academic records. The control of energy consumption is central to SDG7 (affordable and clean energy), and with the blockchain, energy expenditure can be securely and transparently controlled in line with the real needs of users. In order to reduce the inequalities, set out in SDG10, UNICEF has launched its connect project, which is a global blockchain-based platform (https://projectconnect.unicef.org/map) that organises information from each country, and informs its users which schools around the world lack the necessary Internet connectivity, as well as the quality of each school's Internet connection. Finally, the Commonwealth Bank of Australia has developed a prototype platform to facilitate the protection of environmental ecosystems, so that users can purchase BioTokens to participate in an efficient blockchain-based marketplace. (Mattila, Dwivedi, Gauri, Ahbab, 2022, pp. 237-8).

4. 3. Blockchain and Human Rights

BCT has many applications that can enhance the protection of human rights, as Crumpler has pointed out (Crumpler, 2021) in the following contexts: supply chain, voter turnout, digital identity and land rights management. In line with Crumpler's work, he will refer to some of these applications without aiming to be exhaustive, as it is only a question of connecting the virtues of the BCT with the guarantee and protection of human rights.

The possibility of knowing all the links in supply chains thanks to BCT has many practical applications (Bager, Düdder, Hébert, Wu, 2022) (Deshmukh, 2020). For example, BTC enables effective verification of compliance with sustainability criteria, as well as precise knowledge of the origin of materials used in production cycles. BTC can also be very useful in eliminating forced labour, especially in the case of vulnerable groups, as it would allow buyers to know the origin of the products they are able to purchase in the market, and to connect this information with the working conditions of the labour force in charge of producing those products. In addition, BTC provides users with valuable information that allows them to make their consumption decisions knowing the degree of sustainability of production processes. This process would increase user confidence and allow buyers to put pressure on suppliers when they are not environmentally friendly or sustainable.

The quality and quantity of participation in electoral processes can benefit from BCT, especially in the context of voter registration or communication with voters. Blockchain can promote voter participation, especially for those who do not want to vote face-to-face for fear of reprisals. Online voting also has drawbacks, as Crumpler pointed out: "Blockchain-based systems are also limited in that they cannot provide assurance that votes have not been tampered with before being logged on the blockchain. Just as in the supply chain traceability use case, Blockchain would only serve to protect ballots once they are submitted to the network and can do nothing to prevent tampering by government authorities or outside actors that occur at other points in the voting process. Election security researchers have consistently found that the hardware and software used by online voting systems for submitting, receiving, and counting ballots are highly vulnerable to attacks, even when blockchain is used to store the votes. These vulnerabilities could allow both internal and external actors to carry out large-scale disruption or manipulation for a very low cost" (Crumpler, 2021, p. VIII). The key to any proposal in this area is to ensure that data cannot be manipulated at any part of the chain, from the time of voting to the announcement of the election results.

The identification of individuals has traditionally been a task carried out exclusively by states, which issue an identity document whose fidelity was guaranteed by the state itself (as is the case with passports) according to official national documentation, such as civil registration information. The virtual world is not organised around geographical territories or the nationality of the operators; on the contrary, in the virtual world operators choose their identity or pseudonym according to their own interests.

In order to control the identity of users, “trusted third parties” have been created, which confirm the identity of users to third parties on the basis of the information they provide. Trusted third parties, while having the advantage of facilitating data traffic and anonymity, have the disadvantage that it is not clear what uses the platforms that collect the data can make of them. In fact, in most cases the only way to carry out transactions on the Internet is by giving personal information to private platforms, mainly related to address or bank details, which can be stolen by third parties in the virtual world.

BCT makes it possible to obtain digital identification and to act autonomously and anonymously in data traffic. Some groups have difficulties in identifying themselves or lack official documentation, especially refugees and migrants, who could obtain digital identification with the guarantee of international institutions, such as the United Nations. Digital identification would help to combat human trafficking, especially in the case of vulnerable groups as children and migrants, as these people lack official documentation that adequately guarantees their identity. People without identification are excluded from society and cannot act in legal transactions to satisfy their basic needs, such as buying food, for example.

The debate around digital identity focuses on self-sufficient identity (SSI) and the possibility for individuals to self-manage their identity without validation by third parties or entities. The main beneficiaries of the SSI are groups that have difficulties in identifying themselves, such as in the case of refugees, irregular migrants or stateless persons. SSI needs a regulatory framework that guarantees legal certainty, since a vulnerable SSI, with risks to people’s privacy, would generate more harm than benefits (George, Chacko, 2023).

BCT allows people to create an unofficial portable digital identity that can be used, for example, in contexts such as refugee camps to validate medical or educational records. SSI can be validated with humanitarian organisations or NGOs, so that relationships can be organised between people without official documentation and refugee camp administrators. The downside of SSI is that, on the one hand, its validity requires mutual trust between the parties, and in case it is to be used for identification to state bodies, a prior regulatory framework is necessary; on the other hand, access to valid and reliable technological resources is essential to be able to obtain a digital ID, so users need a smartphone to be able to use SSI technology, or rely on third parties to lend them their smartphones.

An excellent example of the applications that BCT can have in the medical context can be found in the need to connect people’s identities with the so-called vaccine passport during the Covid 19 pandemic. This was an international initiative, thanks to which millions of people were able to travel in compliance with a series of medical criteria (George, Chacko, 2023). Digital identity has also been used to design specific programmes to eliminate poverty. The connection between the food programmes and the digital identity of their beneficiaries does not require the use of intermediaries to manage the aid. An example of this type of programme is the “Via 31 Project” in Buenos Aires, which guarantees access to food to those who have been digitally identified, as this type of project directly connects food providers with people in need, eliminating corruption in the distribution of aid (Borrero, 2018). Likewise, alternative identification mechanisms such as iris scanners using BCT are secure, and guarantee the identification of individuals and may be necessary in contexts where it is not possible to use official documentation (G'sell, Martin-Bariteau, 2022, p. 23).

In other words, while the application of blockchain to digital identification allows people without the capacity to officially identify themselves to prove their identity to third parties. However, it has the disadvantage that it requires users to have access to the necessary technological resources and tools, and that the party to whom they are seeking to identify themselves recognizes their SSI.

The last example Crumpler uses to explain the advantages of using blockchain is the management of land rights. As a starting point, it is necessary to bear in mind that in order for this debate to make sense from a human rights perspective, it is necessary for individuals to be able to access property without being discriminated against, especially in the case of vulnerable groups. According to Crumpler, the main virtues of using blockchain in this context are that it would prevent corruption and the risks of mismanagement. This is especially important in countries where land management is still paper-based and land titles have not been digitised, or in which ownership is transferred through informal mechanisms that are not officially recorded, allowing for the destruction or alteration of land titles and corrupt practices. (Crumpler, 2021, p. X). However, as the author makes clear, the use of BCT, while ensuring that property records are correct and making corrupt practices more difficult, is not in itself sufficient to fully ensure transparency and accountability in the management of land rights.

Finally, in order to properly understand the role that BCT can play in the protection of human rights, it has been proposed that applications with this technology carry out a due diligence study prior to its implementation, so that its main advantages and disadvantages for the guarantee of human rights are known (Crumpler, 2021, p. X). For example, the explanatory memorandum of the proposal for a Regulation of the European Parliament and of the Council on crypto-asset markets (and amending Directive (EU) 2019/1937) noted in its impact assessment that the proposal is not likely to have a direct impact on fundamental rights, as listed in the core UN human rights conventions, the Charter of Fundamental Rights of the European Union, and the European Convention on Human Rights (European commission, 2020). The importance of such measures lies in the fact that, as we have seen, although BCT favours the exercise of human rights, it can also seriously jeopardise them, especially in the case of vulnerable and disadvantaged groups.

5. Conclusions

The GDPR came into force in 2018, modifying the previous regulation in 2 aspects of particular relevance: the processing of personal data and the freedom of movement of such data. According to the new regulatory framework, those operating in the European Union, regardless of their nationality, have become data controllers and processors of personal data. Likewise, the new regulation focuses on the design of a legal framework that ensures adequate security and confidentiality of personal data, for which data processors may be required to establish certification mechanisms and data protection seals and marks.

As regards the right to be forgotten, in accordance with the GDPR, the data subject may request the controller to erase personal data concerning him or her without undue delay. The controller has to decide on a case-by-case basis whether to agree to erase the information, taking into account the right to privacy and the protection of the public interest in certain contexts (health, judicial, scientific or historical research), as well as certain fundamental rights, such as the freedoms of expression and information. The exercise of this right depends on the grounds on which the data subject requests deletion, as well as on whether the data to be deleted are (or are not) necessary for the purposes for which they were collected. The right to be forgotten is not unlimited, but an autonomous right that may be denied in certain cases to protect the public interest in specific contexts (health, judicial, scientific or historical research), as well as certain fundamental rights, such as the freedoms of expression and information.

The Court of Justice of the European Union has ruled on the right to be forgotten with a case law that differentiates between the responsibilities of search engines and the website on which the information is stored. The exercise of the right to be forgotten has been addressed mainly to search engines, in those cases in which websites offer information protected by the Internet user's right of access to information. According to this approach, the right to be forgotten can be defined as the right to remove search engine results, when the search is performed using personal data of the person who wants to be forgotten. This right only applies to search engines with domain names associated with EU Member States, as the European Court of Justice has no jurisdiction outside the EU.

In order to protect the rights to respect for private life and to the protection of personal data, search engine operators have an excessive margin of appreciation to resolve conflicts between the right to data protection and the freedoms of expression and information. Search engine operators should decide the above conflicts on a case-by-case assessment, on the one hand, by analysing whether all results obtained after a search based on the name of the data subject are strictly necessary to protect the freedom of information of Internet users; and, on the other hand, claims related to the right to be forgotten should be resolved taking into account the nature of the information in question, the sensitivity of the dissemination of the information for the privacy of the data subject, and the public interest in having the information available.

The presentation of images by search engines in the form of previews may entail an additional interference with the rights to respect for privacy and to the protection of personal data, since it allows Internet users to access information that is complementary and autonomous to the main information. Therefore, users can also exercise the right to be forgotten with regard to images that search engines associate with their personal data.

The case law of the ECtHR can be described as protective of the right to be forgotten. Like the European Court of Justice, the ECtHR has differentiated between the obligations of publishers and creators of information and search engines. The ECtHR has ruled on the need for personal information provided in digital form to be modified to ensure anonymity, taking into account the way in which news is treated, as well as the information it contains.

The ECtHR has established two principles on the anonymisation of personal data. Firstly, if requested by the data subjects, the media are obliged to review their archives and check whether, when an article is to be archived in their digital archive, it is necessary to keep the personal data or to anonymise it, for example by changing the initials of the first names and surnames by an X. In this way, to avoid violating the right to privacy, it is not necessary to delete the article from the newspaper's archives, but only to anonymise the electronic version. And secondly, in this process it is necessary to assess to what extent the rights to obtain from the controller the erasure of personal data and the freedoms of expression and information can be harmonised, depending on when the information to be modified is no longer necessary for the purposes for which it was collected or processed.

Compatibility between the GDPR and BCT is one of the major challenges that Europe will face in the coming years. The main characteristics of the blockchain are: technological security, autonomy of the system, and transparency and anonymity of the operators. These ingredients make this technology perfect for guaranteeing the quality of data and financial transactions, with very important applications in the field of human rights and sustainable development objectives. However, the main virtue of the BCT (anonymity) collides with the exercise of the right to be forgotten and the role and responsibility that the GDPR mandates for data controllers and processors of personal data.

Mechanisms need to be designed to make BCT compatible with the principles of the GDPR, especially in the context of the right to be forgotten and the designation of the data controller in charge of guaranteeing users' rights in the processes. Otherwise blockchain will be a useless technology, because its main virtue (absence of third parties in the processes and anonymity of its users) prevent it from adequately enforcing the GDPR. To this end, formulas have begun to be designed thanks to some projects led by the European Union, that allow the blockchain to be modified to comply with GDPR regulations, but at the same time without eliminating the main hallmarks of BCT.

Funding

This article has been written within the "TRUST - digital TuRn in EUrope: Strengthening relational reliance through Technology" Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 101007820. This article reflects only the author's view and the REA is not responsible for any use that may be made of the information it contains.

Bibliography

AGUINAGA GLARÍA, B. (2022) "La tutela judicial civil del derecho al olvido digital", *Revista General de Derecho Constitucional*, 37.

ÁLVAREZ, C. (2018) *What is GDPR? The EU's new General Data Protection Regulation, Financial Regulations*. Available at https://www.bbva.com/en/what-is-gdpr-the-eus-new-general-data-protection-regulation/ (access 22/2/2024)

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2014) *Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v Agencia Española de Protección de Datos (Aepd) and Mario Costeja González" C-131/12*. Available at https://www.aepd.es/es/documento/wp225-derecho-al-olvido-en.pdf (access 22/2/2024)

BAGER, S., DÜDDER, B., HÉBERT. J.M., WU, H. (2022) "Event-Based Supply Chain Network Modeling: Blockchain for Good Coffee, Blockchain for Good", *Frontiers in Blockchain*, 5.

BARTOLOMÉ PINA, AR., LINDÍN SORIANO, C. (2018) Posibilidades del Blockchain en Educación, *Education in the knowledge society (EKS)*, 19(4), pp. 81-93.

BILBAO BARBERO, MIREYA. (2019) "Blockchain, transparencia para el desarrollo sostenible", *IEEE*, 15, pp. 221-237.

BOIX PALOP, A. (2015) "El equilibro entre los derechos del artículo 18 de la constitución, el "derecho al olvido" y las libertades informativas tras la sentencia Google", *Revista General de Derecho Administrativo*, 38.

BORRERO, A. (2018) *Blockchain y los Objetivos de Desarrollo Sostenible*. Agenda de la Empresa. Available at https://www.agendaempresa.com/93234/opinion-adolfo-borrero-ceoe-ametic-blockchain-objetivos-de-desarrollo-sostenible-ods/

BUISÁN GARCÍA, N. (2014) "El derecho al olvido el nuevo contenido de un derecho antiguo", *El Cronista del Estado Social y Democrático de Derecho*, 46, pp. 22-35.

CARDÓ GUERRA, M. (2018) "El derecho a la protección de datos en la Unión Europea. Nuevo reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016", *Cuadernos Cantabria Europa*, 17, pp. 116-141.

CASTELLO, I. (2021) *Blockchain y protección de datos, ¿incompatibles?* SGRR. Available at https://www.sgrr.es/nuevas-tecnologias/blockchain-proteccion-datos/ (access 07/07/2024)

COMISIÓN EUROPEA (2021) *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Brújula Digital 2030: el enfoque de Europa para el Decenio Digital,* Bruselas, 9.3.2021, COM(2021) 118 final.

CONSEJO ECONÓMICO Y SOCIAL (2017) "El nuevo modelo europeo de protección de datos: principales novedades", *Cauces: Cuadernos del Consejo Económico y Social*, 36, pp. 17-23.

CRUMPLER, W., FLACKS, M., MANDAVILLI, A. (2021) *The Human Rights Risks and Opportunities in Blockchain,* Center for Strategic & International Studies.

DESHMUKH, S. (2020) *3 ways blockchain can accelerate sustainable development*, World Economic Forum.

EUROPEAN COMMISSION (2020) *Proposal for a Regulation of the European Parliament and of the Council on crypto-asset markets, and amending directive (eu) 2019/1937, com (2020) 593 final 2020/0265(cod)*.

EUROPEAN COUNCIL (2019-2023*) Notices from European Union institutions, bodies, offices and agencies, 2019-2023 Strategy on e-Justice, (2019/C 96/04).*

EUROPEAN DATA PROTECTION BOARD (2020) *Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1. Adopted on 4 May 2020*. Available at https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

FERNÁNDEZ HERNÁNDEZ, C. (2023) "Estructura y contenido del Reglamento UE 2023/1114, sobre los mercados de criptoactivos (Reglamento MICA)", *Diario La Ley*, 73.

FERNÁNDEZ VILLAZÓN, L.A. (2016) "El nuevo Reglamento Europeo de Protección de Datos", *Foro: Revista de ciencias jurídicas y sociales*, 19(1), pp. 395-411.

GEORGE, M., CHACKO, M. (2023) "Health Passport: A blockchain-based PHR-integrated self-sovereign identity system", *Frontiers in Blockchain*, 6.

GRIGERA DEL CAMPILLO, S. (2021) "Privacidad y blockchain", *Revista Blockchain e Inteligencia Artificial*, 2(2), pp. 12-20.

G'SELL, F., MARTIN-BARITEAU, F. (2022) *The Impact of Blockchains for Human Rights, Democracy, and the Rule of Law*, Report, Council of Europe.

GUICHOT REINA. E. (2019) "El reconocimiento y desarrollo del derecho al olvido en el Derecho europeo y español", *Revista de administración pública*, 209, pp. 45-92.

HIROYUKI, T. (2019) "What does GDPR mean for blockchain technologies?", *IBM*, February 19th. Available at https://www.thegreengrid.org/en/newsroom/blog/what-does-gdpr-mean-blockchain-technologies

MATTILA V., DWIVEDI P., GAURI P., AHBAB M. (2022) "The Role of Blockchain in Sustainable Development Goals (SDGs)", *International Journal of Management and Commerce Innovations*, 9(2), pp. 231-241.

MENA DURAN, M. L. (2021) *¿Son compatibles el Blockchain y el GDPR?*, The Technolawgist. Available at https://www.thetechnolawgist.com/2021/02/22/son-compatibles-el-blockchain-y-el-gdpr/

MENDOZA ENRÍQUEZ, O.A. (2020) "Blockchain y protección de datos personales", *Informática y Derecho: Revista Iberoamericana de Derecho Informático* (segunda época), 8, pp. 107-120.

MHLANGA, D. (2023) "Block chain technology for digital financial inclusion in the industry 4.0, towards sustainable development?" *Frontiers*, 6. https://doi.org/10.3389/fbloc.2023.1035405

MIERES MIERES, L.J. (2014) "El derecho al olvido digital", *Documentos de trabajo (Laboratorio de alternativas)*, 186.

PIRKOVA, E., MASSÉEU, E. (2019) "Court decides on two major "right to be forgotten" cases: there are no winners here", *Accessnow*, October 23rd 2019.

RECIO GAYO, M. (2020) "Derecho al olvido. Notas sobre su evolución y futuro en la Unión Europea", *El Cronista del Estado Social y Democrático de Derecho*, 88(mayo-junio), pp. 84-95.

REFORM.UK, GDPR AND BLOCKCHAIN. (2018) *Are Blockchain and GDPR compatible? Some issues to consider*, 14th August 2018.

SAMONTE, M. (2019) "Google v CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law", *European Papers*, 4(3).

SANCHO LÓPEZ, M. (2018) "Nuevas tecnologías, Big Data y Derecho al olvido digital: ¿supone el nuevo reglamento europeo de datos personales un cambio de modelo?", *Papeles El tiempo de los derechos*, 7.

SORIANO GARCÍA, J. E. (2018) "Presente del derecho al olvido", *El Cronista del Estado Social y Democrático de Derecho*, 78, pp. 4-21.

TORRES MANRIQUE, J. I. (2018) "Analizando el derecho fundamental al olvido a propósito de su reciente reconocimiento y evolución", *Revista General de Derecho Constitucional*, 27.

WEINSTEIN, JASON (2016) "Why Bitcoin is Better for Crime Fighters than Criminals", *CoinDesk's*, available at https://www.coindesk.com/markets/2016/04/04/why-bitcoin-is-better-for-crime-fighters-than-criminals/ (access 22/2/2024)

ZÁRATE ROJAS, S. (2013) "La problemática entre el derecho al olvido y la libertad de prensa", *Derecom*, 13(mar-may).

Received: 22nd February 2024

Accepted: 9th July 2024