CELE

Implementing “Digital Oblivion”: Forgetting Details

February 2019

Facultad de Derecho
Centro de Estudios en Libertad
de Expresión y Acceso a la Información

UP
Universidad
de Palermo

Implementing "Digital Oblivion": Forgetting Details

Carlos Cortés[1] and Luisa Fernanda Isaza[2]

I. Introducción

"In a connected world, someone's life can be ruined in a matter of minutes and a person stuck frozen in time," says American academic Meg Leta Jones.[3] The Internet offers us examples on a daily basis: a humiliating moment that is captured on a cell phone and multiplies in social networks like a virus; a news scandal that nobody remembers but that persecutes its protagonist every time someone Googles their name; an old tweet that is unearthed to embarrass the author... It seems that the past on the Internet does not exist. We live in an eternal present.

We have been talking about the "right to be forgotten" on the Internet for several years. In a broad sense, this is the power to silence a person's past events; this "right" has been making its way into our region.[4] Its origin is found primarily in the protection of an individual's personal data. The international benchmark that allowed the use of "digital oblivion" took place in Europe: in 2014, the Court of Justice of the European Union decided that the Google search engine should avoid showing old news referred to a person's past debt when searching for their name (known as the "Costeja ruling").

In that ruling, the European justice urged Google to develop a private system whereby European citizens can request the search engine to de-index inaccurate, inadequate, irrelevant or excessive information about them. In general terms, de-indexing implies that the search engine disassociates a particular link from the search results.[5] Between mid-2014 and the end of 2017, Google received requests for de-indexing 2.4 million Internet addresses (URLs), 43% of which were executed. 89% of the cases were undertaken by private citizens.[6]

The Costeja ruling made the search engine liable for guaranteeing "digital oblivion" as opposed to the party which had produced the information or was hosting it. That is to say: according to this decision, the search intermediary must prevent the "harmful" information from being associated with the name of the affected party. The

---

[1] Carlos Cortés is a researcher of the Iniciativa por la Libertad de Expresión [Initiative for Freedom of Expression] (iLEI) of CELE. He is a Lawyer from the Universidad de Los Andes (Colombia), with a Master's degree in Media Governance from the London School of Economics. He is a consultant in freedom of expression and Internet regulation.

[2] Luisa Isaza is a Lawyer from the Universidad Javeriana (Colombia). She is a Legal advisor for the Coordinación de Defensa y Atención a Periodistas de la Fundación para la Libertad de Prensa [Defense and Attention to Journalists Office, Foundation for Freedom of the Press] (FLIP), Colombia.

*The investigation and the elaboration of the document counted with the comments of Agustina Del Campo, CELE's director.

[3] Leta Jones, Meg, Ctrl + Z: The Right to Be Forgotten, New York, NYU Press, Kindle edition, 2016, loc. 105.

[4] Cf. Pino, Giorgio, "The Right to Personal Identity in Italian Private Law: Constitutional Interpretation and Judge-Made Rights", in: Mark Van Hoecke and François Ost (eds.). The Harmonization of Private Law in Europe, Oxford, Hart Publishing, 2000, pp. 225-237.

[5] Although the term "unindexing" is also used, this document chooses to use the word "de-indexation", either partially or as a whole. Part of the purpose of the paper is to make it clear what this action means in each case.

[6] Smith, Michee, "Updating our 'Right to Be Forgotten' Transparency Report", February 26, 2018, retrieved from: https://bit.ly/2SGwtLT.

information still exists, but finding it is much more complicated by not being part of the search results under that person's name.[7]

This precedent has been applied in some administrative and judicial rulings in Latin America. While the private Google de-indexing system is in place in Europe, in our region there are specific cases where an authority gives an equivalent order. In any case, neither the administrative nor judicial authorities in our region have reached the point of ordering the creation of a private system similar to the European one.

In contrast, other decisions in the region focused the responsibility of "digital oblivion" on the author or publisher of the information. As a result, they ordered the responsible party to update or delete specific information. In this scenario, the search engine is not part of the controversy, and if the author of the information eliminates it, this information simply disappears from the search results.

In the midst of these two types of orders, those focused on the search engine and those directed to the publisher, there are combined, intermediate, and openly contradictory decisions. When trying to implement "digital oblivion", the judges of Latin America are going through unfamiliar territory. Understanding the technical implications and exploring their implementation and consequences is the objective of this paper.

It is important to delimit the scope of this analysis: the digital "right to be forgotten" includes several discussions about the need to return control over the data and the information that circulates on the Internet to the individual. In this paper, we want to focus on the "digital oblivion" that impacts the exercise of freedom of expression and, in particular, the activity of the media and those who disseminate information and opinions of general interest. That is to say, "digital oblivion" is not studied in relation to the discussion about the personal information that companies gather and keep in databases. We focus on the orders that resolve conflicts between freedom of expression and individual rights such as the right to a good name, privacy and the free development of personality, due to information that is published openly on the Internet.

This paper focuses on decisions about "digital oblivion" in its broadest sense: those that seek to eliminate, obscure or hinder access to certain information. On the other hand, we do not address other components of those rulings that seek to balance public debate. This is the case of rulings about information update, those that grant a right of reply or those that require the publication of a warning (flagging). It is worth adding, however, that these last rulings do not exclude those pertaining to "digital oblivion" (think, for example, of a provision that requires the elimination of information and at the same time requires granting affected party the space to exercise their right to reply).

Furthermore, this document does not address in a critical manner the concept of the "right to be forgotten" or the legitimacy of the agent that implements it. This has been dealt with in other publications of the Center for Studies on Freedom of Expression and Access to Information (CELE) and in previous works by the authors.[8] We be-

---

[7] It is currently being debated whether the de-indexation measures adopted by Google based on this ruling should be applied only in their European domains (such as Google.fr, Google.es, etc.) or if, on the contrary, there is a right to request a global de-indexation. The Court of Justice of the European Union is close to deciding on a preliminary issue raised by the Council of State of France in this regard after Google sued the National Commission for Information Technology and Liberties of France (CNIL) for having imposed a penalty for limiting the de-indexing to European domains.

[8] *See*, Cortés, Carlos, *"Derecho al olvido: entre la protección de datos, la memoria y la vida personal en la era digital"*, in: Bertoni, Eduardo (comp.). *Internet y derechos humanos. Aportes para la discusión en América Latina*. Buenos Aires, CELE-Universidad de Palermo, 2014; Ferrari, Verónica and Schnidrig, Daniela, "Responsabilidad de intermediarios y derecho al olvido. *Aportes para la discusión legislativa en Argentina"*, in: Bertoni, Eduardo (comp.). *Internet y derechos humanos II. Aportes para la discusión en América Latina*, Buenos Aires, CELE-Universidad de Palermo, 2016; Botero, Catalina, Camilleri, Michael J. and Cortés, Carlos, "*Democracia en la era digital. Libertad de expresión y el derecho al olvido europeo"*, in: *El Diálogo. Liderazgo para las Américas*, Informe del Programa de Estado de Derecho, November, 2017.

lieve that the idea of "digital oblivion" faces many theoretical questions, and that the incorporation of this "right" in the context of the Inter-American Human Rights System should continue to be discussed. On this occasion, we want to focus on the implementation issue.

"Digital oblivion" implies a series of actions on information, data and content: elimination, updating, obscuring and invisibility. These actions can operate on different levels, involve different actors and generate variations in the type of "oblivion". Do judges, administrative authorities and interested civil society understand the implementation of these orders? Are the proportionality and possibility of these orders being evaluated? Are the impact they have and the incentives they generate being analyzed? Do the environment and practices of private companies allow the understanding of technical problems? Is there a transparent and honest discussion about it?

To understand where oblivion actions are implemented, the first part of this paper describes the concepts of transactive memory and open and closed systems. The purpose is to explain, on the one hand, how the closer the method of "digital oblivion" is to the storage core, the more domains will be affected. And, on the other, how that "oblivion" usually involves the action of several players, which cannot be impacted by a single decision or technical measure.

Subsequently, "digital oblivion" is addressed in practice towards the two agents involved: the search engine and the author of the information. In both cases, emphasis is placed on the nature of the orders issued and their possible implementation. Finally, the last part offers some conclusions focused on the problems of proportionality and incentives.

This paper attempts to simplify a complex issue in order to bring the discussion to judicial operators and members of civil society. In that regard, it omits some technical details, but also part of the assumption that the audience has a minimal previous frame of reference on the debate on "digital oblivion".

II. Transactive memory and open and closed systems

Throughout the centuries, human beings have created and perfected techniques and tools that support our perishable memory. The clearest example is the external objects that "memorize" information for us: a phone book, the alarm clock or a post-it with a reminder. In the digital environment, these objects have been replaced by applications and services: phone numbers stored in cell phones, the cell phone's alarm or its list of tasks.

Memory also operates, above all, in cooperation with other people. In our group of friends or colleagues, a decentralized process of storage and consultation is constantly taking place: "I remember that Pablo's birthday is July 15 because that day my niece was born, but I do not remember the date for Felipe's day," someone says. "It's November 19, like the song," someone else replies. In a conversation as simple as this, a transactive memory process is performed, meaning the "combination of individual minds and the communication between them".[9]

Transactive memory refers to how information is coded, stored and retrieved collectively. According to the psychologists who coined the term, transactive memory is defined by two components: (i) an organized storage of

[9] Cf. Wegner, Daniel M., Giuliano, Toni and Hertel, Paula T., "Cognitive Interdependence in Close Relationships", in: Ickes, William J. (ed.). Compatible and Incompatible Relationships, New York, Springer-Verlag, 1985, p. 256. Retrieved from: https://bit.ly/2sf9qMQ, last access: December 28, 2018.

knowledge that is housed entirely in the individual memory systems of the members of the group, and (ii) a set of relevant transaction processes for knowledge that occur between members.

As it is a space in which people can consult or provide information, the Internet is a system of transactive memory.[10] This is relevant to understanding "digital oblivion", what its effects are and who is the agent responsible for taking the necessary measures to "forget". We are not confronted with the external memory of a single agent but multiple agents, each of which may have different interests in the elimination or retention of the information in question. "The problem of fulfilling an individual's need to 'be forgotten' from an external network memory storage is that it is not the external storage of the individual, but a transactive one."[11]

Transactive memories can reside in open or closed access systems. According to Vijfvinkel, in an open system the information can be copied by anyone, without there being the possibility of keeping tags on the copies.[12] This is the case, for example, of an open discussion forum in which anyone can read the information published by its participants. Meanwhile, in a closed system the dissemination of information is limited to controlled spaces, and all its operators are limited by space restrictions and by conventional or legal obligations of non-disclosure.[13] Think about the system for consulting and editing medical records of a hospital's patients.

Vijfvinkel explains that both open and closed access systems operate on different levels: the first is the layer of the physical medium where the data is stored — the "domain of the system" — and the layer where the data can be consulted — the "domain of the organization". In the medical records system, the domain of the system would be, for example, the server where those are stored, and the domain of the organization would be for the members of the medical and administrative personnel authorized for consults. This is the end of access levels in a closed system like this, where there is no space for public consults.

In an open access system, however, there are additional layers where the possibilities of consultation and exchange of information increase. And the more open the access to the system, the more transactive it will be. Facebook, for example, requires user authentication to access its contents, this would be a semi-transactive memory. Wikipedia, which in contrast does not require this authentication neither to consult the contents nor to produce them, would be a transactive memory.

Another example of an open access system of transactive memory, also relevant to this paper, is the one between the web page of a media outlet and the search engine used to locate a newspaper article from a term introduced by a user. Although knowledge is housed in one place — the media outlet's server —, the search engine generates the process so that knowledge is available to enable users to "remember".

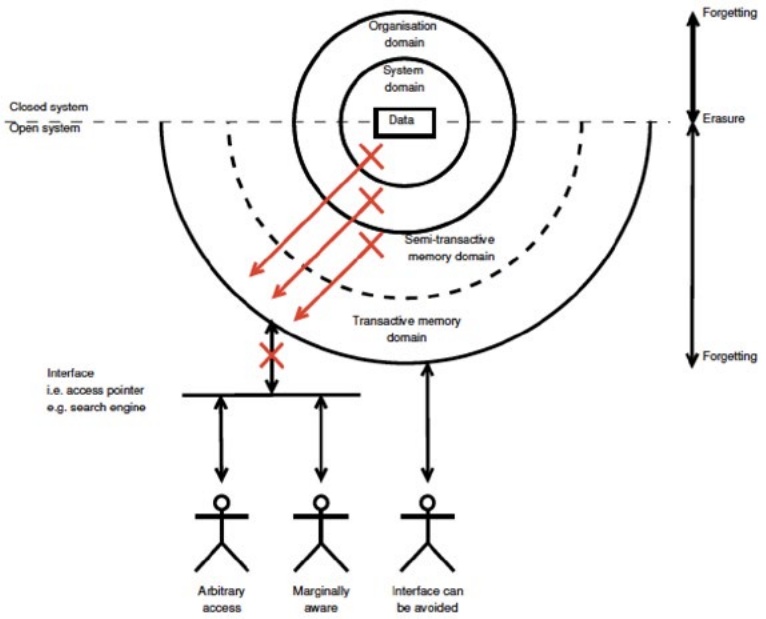
---

[10] The notion of the Internet as a transactive memory was popularized by a famous study published in Science magazine in 2011 that revealed that people tend to forget the information they hope to be able to consult again using the web. Sparrow, Betsy, Liu, Jenny and Wegner, Daniel M., "Google Effects on Memory: Cognitive Consequences of Having Information at Our Fingertips", in: Science, Vol. 333, No. 6043, 2011, retrieved from: https://bit.ly/2xTCB8i, last access: December 28, 2018.

[11] Korenhof, Paulan, Ausloos, Jef, Szekely, Ivan et al., "Timing the Right to Be Forgotten: A Study into 'Time' as a Factor in Deciding About Retention or Erasure of Data", in: Gurwirth, Serge, Leenes, Ronald and de Hert, Paul (eds.). *Reforming European Data Protection Law,* Vol. 20, Dordrecht, Springer, 2015.

[12] Vijfvinkel, M.M., "Technology and the Right to be Forgotten", thesis submitted to obtain the Master's degree in Computer Science, Radboud University, Nijmegen, Netherlands, 2016.

[13] Druschel, Peter, Backers, Michael and Tirtea, Rodica, "The Right to Be Forgotten. Between Expectations and Practice", European Network and Information Security (ENISA), 2012.



"The closer the method of 'oblivion' is to the data storage location, the more domains will be affected," explains Vijfvinkel.

The domain system allows us to understand the type of measures implemented by "digital oblivion": "The closer the method of 'oblivion' is to the data storage location, the more domains will be affected," explains Vijfvinkel.[14] Depending on the layer where the measures are implemented, the effects will vary and be unequal among the users of the information. For example, an order to delete information in the domain of the system — in the digital file of a media outlet, for instance — will affect all other domains and all users. On the other hand, a measure applied to the domain of the transactive memory — a de-indexing order for the search engine — will not affect the information: it will still be available to those users who move in the semi-transactive domain (they are subscribers of the media outlet or they know the access link, for example), or in the domain of the organization (media journalists with access to the server). However, both will have to know how to look for it.

Another important aspect of the domain system is to understand who controls the information and who is really in a position to eliminate it from the system or to control how it is exchanged in a transactive system. Following the previous example, the search engine that indexes Internet pages for the search results cannot modify or delete the information in the domain of the system. On the contrary, if the media outlet that published the article removes it from its servers — that is, from the domain of the system — this will affect the search engine result. However, if that piece of news is available in an open access system, the media outlet cannot control all subsequent actions that are built in the transactive memory: an article published in a media outlet can be shared in screenshots or copied and published in a third-party blog, and very possibly these contents will in turn be indexed by the search engine.[15]

[14] Vijfvinkel, *supra* note 10.

[15] The media outlet would have the possibility to control subsequent actions if it works as a closed access system, for example, in those cases where it has implemented digital rights management measures or anti-copy programs (also known as DRM for digital rights management), through which it can control the access and use of its publications.

III. The "digital oblivion" in practice

Implementing the digital "right to be forgotten" requires entering the engine room of a media outlet or an intermediary. In other words, it means that these agents have to be made aware of the terms in which their service must relate to the content. As we stated in the introduction, many of these decisions are made without taking into account the capabilities and technical consequences. Next, we will provide examples of judicial or administrative decisions to classify and analyze those orders taking into account the responsibility assigned to the two relevant actors: the search engine and the author or publisher of the information. In the latter case, as was already stated, we want to focus on the media, but we will refer to some decisions that center on other agents and that are relevant to the present analysis.

1. Focus placed on the search engine

1.1. De-indexing (total and partial)

In the Costeja ruling, the Court of Justice of the European Union considered that search engines (and Google in particular) carry out the processing of personal data when indexing the websites of third parties. Consequently, they are responsible for complying with European regulations in this matter.[16] And although the court recognized that authors of external content — like the media — can prevent their publication from being indexed by search engines (through measures that will be discussed later), it concluded that this option does not remove liability from search engines, especially when those authors do not respond to the questioned content.[17]

The ruling then states that Google has to adopt the measure of "digital oblivion". The technical instruction given by the court was not very thorough: the search engine is forced to evaluate and, when appropriate, eliminate from the search results — obtained from a person's name — the 'links' to web pages that contain the questioned information.[18] This means that, according to the ruling, Google must not de-index the questioned "link" from the search results completely. It is a partial de-indexation: Google restricts the results of a search associated with a particular name, but maintains the links if other related terms are searched.[19]

Let's illustrate the point with an example: John Doe is a citizen who several years ago was involved in the crime of tax evasion, this piece of news was reported by a local media outlet and it appears indexed as Google's first

[16] Tribunal de Justicia (Gran Sala), "Google Spain, S.L., Google Inc. vs. Agencia Española de Protección de Datos (AEPD), Mario Costeja González", judgment, May 13, 2014, retrieved from: https://bit.ly/2sug3Nu, last access: December 28, 2018.

[17] The court justified the search engine's liability stating that: (i) the author of a web page can benefit from the exception that protects the processing of data for journalistic purposes, (ii) including this content in the results of a search of someone's name enables any Internet user to access this information, which represents a greater breach in privacy than the one carried out by the author of the web site, and (iii) since the information can be copied easily by sites that are not subject to European Union law, effective protection of data owners could not be achieved if they had to resort to such websites.

[18] According to the court, the decision must be made in relation to "links" to web pages with truthful information, legitimately published by third parties, when said information is "inadequate, not pertinent, or is no longer pertinent, or is excessive in relation to the purposes of the treatment in question carried out by the search engine". And the judgment states: "The manager of a search engine is obliged to remove from the list of results obtained after a search made of the name of a person links to web pages published by third parties and containing information relating to this person, also in the event that this name or this information is not previously or simultaneously deleted from these web pages, and, if applicable, even if the publication on said pages is in itself lawful."

[19] The European court requires that partial de-indexing be made in all European domains of Google Search (Google.fr or Google.es) and even searches from non-European domains that are made within the territory of the person who requested the measure of "digital oblivion".

search result when typing his name. Following the criteria established by the Costeja ruling, the information about Doe is excessive and inadequate, so Google must partially de-index the news: when someone types "John Doe" that result should not appear in the search engine. But if someone performs a search and uses different terms ("tax evasion" and the year or city where the event occurred), the result is still available.

Based on the precedent set by the Costeja ruling, other courts in our region adopted analogous or similar criteria. In 2014, for example, Mexico's data protection authority issued a partial de-indexation order for media information.[20] The administrative authority ordered Google Mexico to refrain from "treating the personal data of the Holder, consisting of their name and surname, in such a way that, when said name is typed into the search engine of the Responsible Party, the links or URL (indexation) do not appear as was requested by the Holder".[21] In 2016, the decision was annulled by a court protection known as *amparo*.[22]

The orders issued by the European court and the Mexican authority are directed to the search engine and not to the author of the website that published the information, which puts us in the domain of transactive memory. The measure of "digital oblivion" does not affect internal domains: the information will remain available for those who have the direct "link" to the article or for those who perform a search on the same web page of the media outlet, but will not be available via a Google search of the name of the person affected.

1.2. Degradation of the search ranking

A well-known Internet "meme" says that the best place to hide a dead body is page two of Google's search results. Why is this so? Nobody will look for it there. According to a 2014 study, 95% of a search engine's traffic is concentrated on the first page of results.[23]

Following this logic, the Privacy Commissioner of Canada recently proposed that search engines be forced to remove certain "links" in the ranking of search results as a way of protecting the reputation of people on the Internet.[24] However, to date this solution has not been ordered by any authority.

---

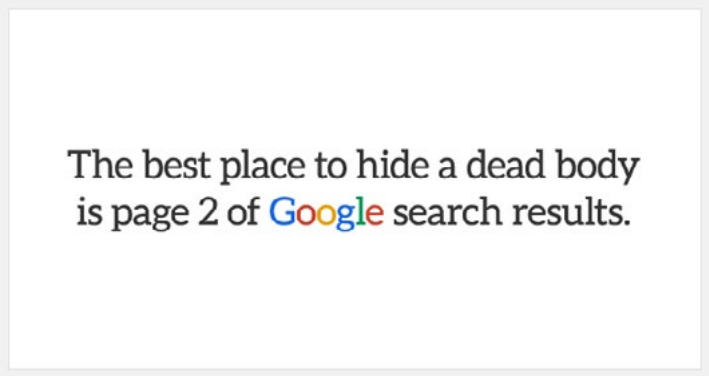
[20] The authority is the *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales* [National Institute of Transparency, Access to Information and Protection of Personal Data], (INAI).

[21] INAI, file: PPD.0094/14, Responsible Party: Google México, S. de R.L. de C.V., 2014, retrieved from: https://bit.ly/1jr0U6E, last access: December 28, 2018.

[22] *"¡Ganamos! Tribunal anula resolución del INAI sobre el falso 'derecho al olvido"*, Red en Defensa de los Derechos Digitales, August 24, 2016, retrieved from: https://bit.ly/2VCS0qW, last access: December 28, 2018.

[23] Jacobson, Madeline, "How Far Down the Search Engine Results Page Will Most People Go?" in: *Leverage Marketing*, August 14, 2017. Retrieved from: https://bit.ly/2scfc1F, last access: December 28, 2018.

[24] Office of the Privacy Commissioner of Canada (OPC), "Draft OPC Position on Online Reputation", January 26, 2018, retrieved from: https://bit.ly/2CU0rXg, last access: December 28, 2018.



""The best place to hide a dead body is page two of Google's search results."

This solution would have an impact on the domain of the transactive memory, although with a different effect than the partial or total de-indexing, since the "link" is kept up, even if the name of a person were searched. The question would be if this form of "hiding" the "link" would work for any search or if, like in the case of the European ruling, its ranking was lowered only when searching for the name of the person concerned. For the moment, this proposal has not been further developed.

2. Focus placed on the author or publisher

2.1. Removal

In January 2016, the Third Chamber of the Supreme Court of Justice of Chile ordered a media outlet to "eliminate the digital record of the news that adversely affected the appellant, within a period of three days."[25]. The information had been published ten years earlier, and referred to the participation of a citizen of unusual surname in a crime. Once the sentence was served, the citizen requested the elimination of the information arguing that the news was no longer relevant.

According to the Court, if criminal law indicates the duration of a penalty and allows its elimination from public records once it is complied with, it is consistent that the media do the same and thus allow the individual's social reintegration.[26] The Court argues that maintaining that digital registry does not report any benefit for freedom of expression and in any case the information "can be consulted by analogous methods through professional investigative exercise by whoever is interested in it". In any case, the Court clarifies that this is not about removing information from all digital records, but that access to it is limited to official sources and to the terms set forth in the law.

The agent in charge of implementing the order is the media outlet that originated the information. And that's what the Chilean media outlet did: it eliminated the news about the citizen's criminal conviction.[27] The elimination

[25] Corte Suprema de Justicia de Chile [Supreme Court of Justice of Chile], judgment of January 21, 2016, retrieved from: https://bit.ly/2MbDW6m, last access: December 28, 2018.

[26] Justice María Eugenia Sandoval voted against the decision, she stressed that the news dealt with a topic of public interest.

[27] From a technical perspective, the absolute suppression of information from a system is not as simple as it seems. Different methods have been proposed to ensure the irrevocability of the removal, ranging from the destruction of the physical medium and overwriting it to the encryption of the information with the subsequent elimination of the keys.

of information is the most radical measure of "digital oblivion". If it is applied where the data and information are stored — in the domain of the system — it impacts all other layers and affects all users. On the other hand, if the elimination applies only to public access, the information will remain available to those who move within the domain of the organization (that is, the information is maintained in a closed system).

Without overlooking the radical nature of the measure, it is important to bear in mind that as it is information that was part of an open system, the elimination in the core does not cover other downstream locations where it would have been replicated, such as a blog or a social network. These arenas exceed the control that the publisher or author initially had over the information. A judicial or state order cannot then expect the originator of the information to respond technically to these publications, with different actors in control. Furthermore, if the media outlet took the information from another publication — that is, if the domain of the original system is a different one — the act of elimination will only affect its republication orbit.

A complementary Colombian judicial precedent allows us to better understand the limitations inherent to the elimination order. The case originates with an unpaid debt. In 2014, "Esther" decided to publicly expose "Lucía" on Facebook for an unpaid loan.[28] In a common practice of online humiliation — known as online shaming — "Esther" published a photo of "Lucia" in which she denounced the debt and her refusal to respond to messages and calls. After the creditor refused to withdraw the publication, "Lucía" filed an appeal for court protection known as "*tutela*". Although "Lucia" did not deny the existence of the debt, the Constitutional Court approved the request for protection. According to this court, the publication of this information on Facebook put "Lucía" in a state of defenselessness and violated her rights to privacy, good name, image and honor. Consequently, "Esther" had to eliminate the image, the message and publish a public apology.

The removal carried out by "Esther" affected the domain of the Facebook system: once deleted, these contents cannot be recovered or extracted by a third party. However, screen captures and information related to the debt that has been exchanged in other spaces — a very common practice in social networks — will not be affected by the elimination at the source and, therefore, will not be impacted by the court order.

2.2. Pseudonymization

In 2014, a Colombian citizen filed a court protection known as *amparo* against the Supreme Court of Justice for publishing on its website information about her related to a criminal conviction for the crimes of extortion, falsehood in a public document and procedural fraud. The claimant had already served her sentence, but this precedent was easily accessible by searching her name on Google.

The Constitutional Court accepted the citizen's claim. The Court argued that, although enforceable sentences are governed by the principle of publicity, they must be subject to the general framework of data management. The Court stated that maintaining certain data available for consultation on the Internet violates the principles of purpose limitation, of restricted access and circulation of data. To that extent, a parallel system of judicial background consultation was being created outside the existing controls on the matter. The Constitutional Court then ordered the Supreme Court of Justice to replace the name of that person with a succession of letters or numbers that would prevent her identification in the public versions of the sentence found on the Internet.[29]

---

[28] The Court modified the names of the protagonists to preserve their privacy.

[29] Corte Constitucional de Colombia [Constitutional Court of Colombia], judgment T-020, January 27, 2014. Judge writing for the court, Luis Guillermo Guerrero, retrieved from: https://bit.ly/2AAZ3as, last access: December 28, 2018.

This decision of the Colombian court is an order of pseudonymization, which consists of hiding the real name of a person, by changing it for another or by making only its initials public. An order of this type must be executed by the author of the website, and would operate in the domain of the system if it is applied to all versions of the document. On the contrary, it would be limited to the domain of the organization if an integral version of the document is kept for its members, but a pseudonymous version is made public.

Pseudonymization already existed in the media as a form of protection of sources and subjects mentioned in newspaper articles. This self-regulatory measure, deployed voluntarily by the media from its operational capacity, could prevent an eventual request of "digital oblivion". By protecting an identity from the beginning, the media outlet decides to avoid exposure of an individual. Depending on how it is implemented, this measure could operate in the domain of the system or the organization.

Although this order was not addressed to a media outlet, it is relevant because of the type of precedent it establishes for journalistic activity. On the one hand, searching for information of public interest about a citizen becomes more difficult. In fact, after this ruling and similar requests, the Supreme Court generalized the rule: when it is proven that a sentence was served or has prescribed, the names of the people in open access databases must be suppressed.

According to the decision, "the condemnatory sentences issued by the Court or the files which references them (...) will be offered in full to the community on its public access server", with the defendant's full names. However, "when it is proven that the sentence has been served or has prescribed; the names of the convicted persons shall be removed from open access databases, except where the law requires that such information be kept public in all cases".[30] The Court maintains that this version will not affect the internal files of the entity, which may be physically consulted according to the rules of access to information. Following the classification proposed in this paper, it is a decision that affects the transactive-memory system, but not the domain of the system or the organization.

2.3. De-indexing (total and partial)

In August 2000, the Colombian newspaper El Tiempo published the article "*Empresa de trata de blancas*", where it reported that the citizen "Gloria" — as she was identified in the file — had been linked, among others, to a criminal investigation for the crime of human trafficking. In 2013, "Gloria" filed a request for a court protection known as *amparo* against El Tiempo and Google, since the process against her had ended by prescription and the news was still published — easily accessible with Google. In 2015, the Constitutional Court of Colombia heard the case.[31]

The high court ruled out two solutions before resolving the case. On the one hand, it released the search engine from any liability, thereby setting a precedent against the Costeja ruling. According to the Court, forcing Google to de-index search results would turn it into a content censor. This could jeopardize freedom of expression and information and affect the architecture of the Internet. On the other hand, and also from the perspective of freedom of expression, the Court considered that an order for the elimination of content did not conform to national and international standards.

It was clear then that the Court was going to center the responsibility on the content's author. However, the Court claimed that an update of the article (with the introduction of the clarification that the criminal action had

[30] Corte Suprema de Justicia [Supreme Court of Justice], judgment August 19, 2015. Justice writing for the court: Patricia Salazar Cuéllar. Abstract of record retrieved from: https://bit.ly/2Rydi9Q, last access: December 28, 2018.

[31] Corte Constitucional de Colombia [Constitutional Court of Colombia], judgment T-277, May 12, 2015. Justice writing for the court: María Victoria Calle, retrieved from: https://bit.ly/1iQCR1b, last access: December 28, 2018.

prescribed in favor of "Gloria", for example) was insufficient to avoid stigmatization. Therefore, it ordered the media outlet that, in addition to the update, it had to take measures so that the search engine did not index that content when a search for the name "Gloria" was made.

It is a partial de-indexation order equal to that of the Costeja ruling, but placing the liability on a different agent. In this case, the court requires the media outlet to instruct the search engine not to index a specific website on its site when searching for a name. The effect should be the same as with the European precedent: the news should be hidden in the Google results if the claimant's name is searched ("Gloria Pérez", for example), but it must be shown for other terms related to the information ("human trafficking in Colombia "). However, that the liable actor is the media outlet and not the search engine has technical implications that were not foreseen by the Court.

The order issued by the Court is technically inaccurate. The ruling provides that the media outlet, "through the technical tool 'robots.txt', 'metatags' or another similar tool, should neutralize the possibility of free access to the article "*Empresa de trata de blancas*"' just by typing the plaintiff's name in the Internet search engines".[32] The problem is that the "robots.txt" protocol, the use of tags or another similar tool, do not allow partial de-indexing that excludes certain words from the content of a "link". The use of these protocols do allow for indexing instructions to the search engine, but in a different sense.

2.3.1. "Robots.txt" and "metatags"

The robot exclusion protocol — known as the "robots.txt" protocol — is the way in which a website informs search engine's crawlers which pages of their website someone does not want to be indexed. That they are not indexed implies, in principle, that they will not appear in the search results under any search term.[33] That is to say that the consequence is a total de-indexation.

The "robots.txt" protocol emerged as a technical response for those website administrators who wanted their content to have a certain degree of privacy without necessarily being secret. In the same way that two people can have a conversation in a public place that can eventually be heard, a web page that does not want to be indexed wants to remain relatively hidden, but not entirely private.[34] American scholar Jonathan Zittrain explains

---

[32] At this point, the Court accepted the search engine's argument: "In this regard, the Court takes note of the response given by Google Colombia Ltda., which states that through the use of tools such as techniques like 'robots.txt' 'and' metatags' it is possible for the owners and administrators of a website to prevent specific contents from being displayed as results when making a query through an Internet search engine. In relation to this issue, the claimant states that by using the tool robots.txt what is achieved is that certain content is not tracked by the search engine. However, despite the use of this tool, the search engine continues to recognize that the information exists and, therefore, may show the title of the article or URL in the search results, even when it could not be accessed because the content was not indexed. Similarly, in relation to the use of metatags, it states that '(...) what is achieved is that a certain URL, despite being indexed, is not shown as a search result'".

[33] We say "in principle" because the search engine could still include in its results pages that "robots.txt" indicated it not to include. This happens when many other third-party sites — which were indexed — include that link in their content, which the algorithm considers to be a relevant result. In this case, the link to the site in question will appear in the list of results, but without the description that usually accompanies it. With this measure it will not appear as a direct consequence of the content found on that site, but indirectly because it has been externally referenced on account of this content. Technically, it is not about "indexing" but about "listing". From Valk, Joost, "Preventing your Site from Being Indexed, the Right Way", June 2017, retrieved from: https://bit.ly/2AyaCiG, last access: December 28, 2018.

[34] According to Zittrain, the lesson of "robots.txt" is that the creation of a basic and simple standard can mean a significant advance in solving or anticipating a problem with important ethical and legal dimensions. Zittrain, Jonathan, "Privacy 2.0", in: University of Chicago Legal Forum, Vol. 2008, article 3, 2008, p. 104

that “robots.txt” is not an official standard: there is no guarantee that current or future crawlers will respect it.[35] However, in the self-regulatory and consensual logic of the Internet, the most popular search engines accept the non-indexing requests included in “robots.txt”.[36]

“Robots.txt” works through a text file that is inserted in the root of the website and which includes the web addresses (URL) that have to be de-indexed. The exclusion of the URL is complete: it is not possible, and this is important to reiterate, to define parts of a page that should be indexed and others that cannot be indexed. If we assume that the search engine is a large telephone directory, “robots.txt” only allows you to request that an apartment in a particular building not be listed, but it does not allow you to choose in which cases the apartment should appear and in which it should not.

```
User-agent: *
Allow: /ads/public/
Allow: /svc/news/v3/all/pshb.rss
Disallow: /ads/
Disallow: /adx/bin/
Disallow: /archives/
Disallow: /auth/
Disallow: /cnet/
Disallow: /college/
Disallow: /external/
Disallow: /financialtimes/
Disallow: /idg/
Disallow: /indexes/
Disallow: /library/
Disallow: /nytimes-partners/
Disallow: /packages/flash/multimedia/TEMPLATES/
Disallow: /pages/college/
Disallow: /paidcontent/
Disallow: /partners/
Disallow: /register
Disallow: /thestreet/
Disallow: /svc
Disallow: /video/embedded/*
Disallow: /web-services/
Disallow: /gst/travel/travsearch*
Disallow: /1996/06/17/nyregion/guest-at-diplomat-s-party-accused-of-rape.html
Disallow: /*.amp.html$

User-agent: googlebot
Allow: /*.amp.html$

User-agent: bingbot
Allow: /*.amp.html$

User-Agent: omgilibot
Disallow: /

User-Agent: omgili
Disallow: /

Sitemap: https://www.nytimes.com/sitemaps/www.nytimes.com/sitemap.xml.gz
Sitemap: https://www.nytimes.com/sitemaps/sitemap_news/sitemap.xml.gz
Sitemap: https://www.nytimes.com/sitemaps/sitemap_video/sitemap.xml.gz
Sitemap: https://www.nytimes.com/sitemaps/www.nytimes.com_realestate/sitemap.xml.gz
Sitemap: https://www.nytimes.com/sitemaps/www.nytimes.com/2016_election_sitemap.xml.gz
```

“Robots.txt” page from nytimes.com. The “disallow” command instructs to not index a particular URL.

On the other hand, “metatags” are labels (in a programming code known as HTML) that are used to record important information about a website: the description of the page, the keywords and the author’s name, among others. This information is included in the page header code and not in the body of the page, so it is information invisible to the user. Using “metatags” and “robots” with values as “noindex” or “nofollow” can give directions by

---

[35] *Ibid.*

[36] On the Google search help page, see *“Información sobre los archivos robots.txt* [Information about robots.txt files]” in the section *“Cómo bloquear URLs con robots.txt* [How to block URLs with robots.txt]”, retrieved from: https://support.google.com/webmasters/answer/6062608, last access: December 28, 2018. In Yahoo, consult *“Elimina tu sitio web del* índice *de búsqueda* [Remove your website from the search index]”, retrieved from: https://es.ayuda.yahoo.com/kb/SLN2214.html?guccounter=1, last access: December 28, 2018. In Bing, “How to Create a Robots.txt File”, retrieved from: https://binged.it/2FcaCcc, last access: December 28, 2018.

using labels or categories, for example, to prevent one or more URLs to be indexed or tracked by search engines.[37]

Both "robots.txt" and "metatags" do not allow compliance with the order of the Colombian court. Nor do other "similar" tools seem to exist — as the court suggests — to achieve partial de-indexation. In specialized circles, there is a mention of tags that allow the search engine to be instructed not to index some parts of a web page.[38] These tags, however, have so far not been recognized by Google nor are they present in the technical forum on the solutions. And, in any case, it is not about tools that allow someone to dictate to the search engine under what words it can list or index the content.[39]

Bearing this in mind, what was the solution in the Colombian case? Faced with an order that could not be met technically, El Tiempo opted simply to use a pseudonym for the claimant's name: "The Prosecutor's Office has just captured 16 people accused of committing the crime of human trafficking and conspiracy to commit a crime, including Ms. Gloria", reads a section of the new version of the text.[40]

IV. Unwanted effects of technical ignorance

One of the theoretical questions faced by "digital oblivion" is the proportionality of its protection. In relation to the right to information, a measure is proportional when it "does not imply a cost for freedom of expression greater than the benefit achieved"[41] Therefore, the objection is that a de-indexation order aimed at protecting the privacy or reputation of a person may end up disproportionately affecting access to general interest information.

There is a risk that the implementation of a technical order will cause unforeseen effects, especially when this does not take into account the praxis of the digital environment and the context in which it must be executed. That is the problem that we identify in our region: the risk of not understanding the technical implications of an order can lead to disproportionate decisions or an incentive for self-censorship. Faced with contradictory or technically impossible decisions, a media outlet may opt, at best, to modify texts of the journalistic archive beyond the scope of the judicial mandate. And, at worst, it may simply prefer to delete the information.

The Colombian precedent of the "Gloria" case brings into the spotlight the problem of not taking into account the technical orbit. Similarly — but in a more worrying aspect — the Peruvian data protection authority has been making decisions about "digital oblivion" without an adequate technical basis. In a recent order against the newspaper El Comercio, the authority of Peru ordered the updating of the headline of an article, but it also seems to

---

[37] Google Webmaster Central Blog, "Using the robots meta tag", 2007, retrieved from: https://bit.ly/2AvMRHV, last access: December 28, 2018. Wikipedia, "Noindex", retrieved from: https://bit.ly/2CX37Uh, last access: December 28, 2018.

[38] Wikipedia, "Noindexing Part of a Page", retrieved from: https://bit.ly/2LVC9z9, last access: December 28, 2018.

[39] We cannot say categorically that there is no possible technical solution. The certain thing is that at this point and with the tools and knowledge within our reach we did not find an answer, which says a lot about how difficult a media outlet would find complying with an order of this nature.

[40] *"Empresa de trata de blancas"* [The human trafficking industry], *El Tiempo*, 2015, retrieved from: https://bit.ly/2AB6H4S, last access: December 28, 2018.

[41] Botero, Camilleri and Cortés, *supra* note 6. This is the standard of the inter-American system according to which limitations on freedom of expression in a democratic society must not only be necessary, but also strictly proportional. According to the Inter-American Court of Human Rights, the sacrifice inherent in the limitation of freedom of expression must not be excessive compared to the advantages derived from the limitation of this right (Kimel v. Argentina case, judgment of May 2, 2008, § 83).

assume that it is the media outlet that carries out the indexing.[42]

In addition to the underlying problems of these decisions — which tend to impact corruption allegations that have not been judicially settled — the rulings are encouraging the media to choose to eliminate content to settle a judicial controversy.[43] In the face of confusion and ambiguity, journalism finds a defense strategy in content subtraction.

The actions to guarantee "digital oblivion" implemented directly in the newsrooms should not be ruled out. There should be new alternatives that are less burdensome for freedom of expression and the journalistic exercise. One of them would be, for example, that the media outlet publishes both a partial — or pseudonymous — version of the article and a complete one. While the first would be indexed by the search engine, the second would include some non-indexing instruction.[44] That the full version is not indexed by the search engine would partially affect the transactive memory: the information cannot be found if the name of the person is searched, but by other related terms because it would refer to the partial or pseudonymous version. However, it would allow preserving it in the domains of the system and the organization of the media outlet (something which apparently did not happen in the final resolution of the "Gloria" case). In other words, the solution would not lead to the total removal of information or its unavailability for open access.

This type of solutions should be analyzed bearing in mind the reality of the newsrooms, since executing them would demand the reorganization of internal processes and a certain degree of progress in programming. They are not, of course, tasks impossible to carry out. A generalized order can generate high costs or entry barriers for the generation and dissemination of information.

V. Conclusion

In addition to the already complex question of what is the "right to be forgotten" and what is its scope in the digital environment, we have the technical questions of how to guarantee this right and what would be its effects. This paper tried to approach the issue of its implementation.

---

[42] It states: "Said update was placed below the article's headline, which causes the Internet search engine Google to render this headline as the first result of a search for the claimant's name, because "El Comercio" had indexed the article's headline". *Dirección de Protección de Datos Personales, Ministerio de Justicia y Derechos Humanos de Perú* [Directorate of Protection of Personal Data, Ministry of Justice and Human Rights of Peru], directorial resolution No. 453 of March 12, 2018.

[43] A Google search with the headline of the aforementioned case — "*"Renzito: ex asesor ministerial sería uno de sus testaferros"* [Renzito: former ministerial advisor is allegedly one of its front men]" — allows us to verify this. Additionally, it does not appear in the newspaper's digital file of the original publication date. See, https://bit.ly/2TwOpsn, last access: December 28, 2018. The information, nevertheless, continues to exist, since other portals copied it. This is an example of content that was in the domain of the transactive memory and that, therefore, subsists despite the removal. This type of solution is not the exception in the media. Last June, one of the authors of this paper spoke in Lima with lawyers and journalists from various media outlets regarding the matter. Several of them accepted that the removal of content has become a form of defense against administrative orders of "digital oblivion".

[44] These two versions could be used to produce a system of partial de-indexing performed by the media outlet that is less restrictive for freedom of expression. As was stated in the paper, the version indexed in Google would be one with partial or pseudonymous information. However, when someone clicked on that link, the page could redirect the user to the complete information that was not indexed by the search engine. These types of redirecting instructions are very common in Internet browsing. Thus, if someone searches for "Gloria" using her own name, the news will not appear in the Google results. But if someone searches for "human trafficking", the modified article would be indexed and, when clicked, would redirect the user to the complete information. This idea came from a conversation with the Colombian programmer David Avellaneda.

Approaching this issue from the transactive memory and the information domains underlines two relevant analysis elements: (i) the closer the method of "digital oblivion" is to the storage core, the more domains will be affected and, therefore, the greater the restriction on freedom of expression and access to information, and (ii) in many cases "digital oblivion" encompasses a "memory" that is constructed collectively among many parties.

The technical approach offers elements to understand the proportionality of the concrete dimension of the impact of a judicial or administrative order, and allows us to understand that, in practice, there is no absolute solution for "digital oblivion". When establishing the role played by the State in promoting technological changes that respond to social expectations, judges and administrative authorities must consider this part of the discussion for decision making.

However, the participation of the State and civil society in this debate requires greater transparency on the part of Internet intermediaries and, in particular, search engines. Talking about the technical implications of a decision is often confused with the inevitability of a present configuration or the impossibility of promoting changes. However, the goal is to identify the starting point to find alternatives. In that process, the responsibility of Internet intermediaries in the design of the algorithms cannot be ignored: "While the algorithms represent calculations and processing that no human could do alone, ultimately humans are the arbiters of the inputs, the design of the system and the results".[45]

Adding the issue of the implementation of "digital oblivion" to the main discussion will also allow seeing it in the context of the impact of the measures taken to achieve technological oblivion and the need for them. That is to say, this will also enable a conversation around caution. "The question about memory and oblivion is not a question that must be solved by a specific date, but one that society must keep open for future generations to decide according to their own circumstances."[46] In the midst of the fragile present and our countries' conflictive past, keeping this question open is even more relevant.

[45] Caplan, Robyn et al. "Algorithmic Accountability: A Primer", in: *Data and Society*, April, 2018, p. 10.

[46] Thouvenin, Florent et al. "Remembering and Forgetting in the Digital Age. A Position Paper", Open Repository and Archive, Zurich, University of Zurich, March, 2016, p. 5. This document is the basis of a book with the same name published in 2018.