

Right to Be Forgotten: Redundancy or Necessity in the Context of Cyberspace?

In the present day, the Internet is the largest provider of information in the world. One could reasonably find any piece of information they desire – from the latest news of the day, through encyclopaedias, to personal information about nearly any individual. According to a special report issued in January 2018, more than 4 billion people have access to the Internet¹. With more than half of the world population being online, the distribution of information has become faster and easier than ever before. However, in spite of all the advantages this information era brings, there exist numerous negatives as well. For one, personal information is often shared by individuals online without them realizing the large-scale consequences its circulation may bring. What is more, once specific data starts circulating in cyberspace, chances are that it will immediately reach a number of other users and will have a certain impact on them which could not be reverted, even if that data is taken down in a matter of minutes.

Once people realized that what they put up online may have destructive consequences in their future, the need emerged for a tool to delete information which they no longer want to be accessible by the public. In the European Union, this need was answered through the introduction of ‘the right to be forgotten’ in the General Data Protection Regulation, drafted in 2016². The right to be forgotten represents a powerful instrument, allowing an individual to request from a controller to delete all personal information, solely on the basis of that individual’s desire and without the need of any reasoning³. The introduction of this piece of legislation, however, was met with mixed feelings. Its defenders see in it a possibility for individuals to not bear the consequences of old and irrelevant information which no longer serves a beneficial purpose online. Its opponents on the other hand, view the right to be forgotten as a tool to manipulate reality for one’s own benefit – a mechanism which, if used accordingly, can bring about serious and extremely large-scale effects.

This essay is going to examine the right to be forgotten as it is codified in the General Data Protection Regulation (hereafter GDPR), while also taking into account the preceding

¹ ‘Internet Usage Statistics’ Internet World Stats, Miniwatts Marketing Group, 30 June 2018
<www.internetworldstats.com/stats.htm>

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) [2016] OJ L119/1

³ Ibid, Article 17(1)

legislation on the matter (namely, the Data Protection Directive⁴) and the historical development of the right. Further, it will discuss the advantages and the disadvantages such legislation would bring to individuals and to society as a whole. In the end, it will be assessed whether a right to be forgotten really is a necessity or a redundancy in the context of cyberspace.

The right to erasure, currently also known as the right to be forgotten, is codified in Article 17 of the GDPR and entails, ‘the right to obtain from the controller the erasure of personal data [...] without undue delay’, and an obligation on the side of the controller, ‘to erase personal data without undue delay’ where such erasure is requested⁵. Up until the introduction of the new Regulation, the right to erasure was codified in Article 12 of the Data Protection Directive (hereafter DPD) which entered into force in 1995⁶. According to it, a data subject has the right to obtain from the controller, ‘erasure [...] of data [...] in particular because of [its] incomplete or inaccurate nature’. The most considerable difference between the right provided in the DPD and its updated version in the GDPR is the lack of a requirement for justification in the newer legislation⁷. The right to erasure as formulated in the Directive has a more limited scope in the sense that such erasure may be allowed only when the information at hand is ‘incomplete or inaccurate’. In other words, one could not require data to be deleted exclusively on the basis of their unwillingness to have this data shared online. The Data Protection Regulation on the other hand provides precisely this. Article 17 allows the data subject to acquire deletion of information without them having to justify their wish, as long as it does not gravely intervene with the freedom of expression or is in another way contrary to the general public interest⁸.

The introduction of the new right to erasure in the General Data Protection Regulation has a notably broader scope than its predecessor, thus giving many more possibilities to data subjects to collocate with their personal information. Undoubtedly, this more extensive freedom brings with itself a number of advantages to Internet users. For one, the right to be forgotten has the capability to ‘delete’ an individual’s past, if not in real life, than at least online. Every person shares information online, the revelation of which they might regret at some point

⁴ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31

⁵ General Data Protection Regulation, Article 17

⁶ Data Protection Directive, Article 12

⁷ Cesare Bartolini and Lawrence Siry, ‘The right to be forgotten in the light of the consent of the data subject’ [2016] 32(2) Computer Law and Security Review 224

⁸ General Data Protection Regulation, Article 17(3)

in their lives. Arguably the most widely known case in this regard is that of Stacy Snyder – a young woman from the United States who was denied a position in an educational institution because of a picture found online by one of her supervisors, portraying her drinking alcohol at a party⁹. It is an undeniable fact that at a younger age, one makes certain decisions and acts in a certain way which might be seen as frivolous and unprofessional at a later stage in their lives. It is equally indisputable that actions of such kind do not define one's personality, and even less their working ethic. Nevertheless, superiors often tend to be prejudiced when such information surfaces about a specific individual. The implementation of the GDPR right to be forgotten is capable of preventing misguided judgements and wrongful stigmatizing, thus allowing individuals to keep their past and their present strictly apart.

Another beneficial consequence of the establishment of the right to be forgotten is that it acts as an additional development of the right to respect for private and family life, as codified in Article 8 of the European Convention on Human Rights¹⁰. Details around an individual's life, in this number also their personal information, are a part of their private life and as such, it follows logically that one should have the right to have them at their disposal in a way they find suitable. Because of its remarkably broad scope but a relatively restricted wording, Article 8 ECHR needs further legislation to specify cases which ought to be regulated. Article 17 GDPR represents precisely such a clarification – the right to be forgotten provides for an extension of the right to respect for private and family life and a way to keep up with it in the rapidly developing cyberspace.

As incontestable and beneficial as the abovementioned characteristics of the right to be forgotten may be, its codification carries with it a large number of disadvantages, some of which are potentially detrimental on a world-wide scale. To begin with, implementation of a right of this kind might prove to be too big a clash with the right to freedom of expression as codified in Article 10 of the European Convention on Human Rights¹². Indeed, Article 17(3)(a) of the GDPR encompasses an exception to the right of erasure specifically when it is in

⁹ Randall Stross, 'How to Lose Your Job on Your Own Time' The New York Times, 30 December 2007 <www.nytimes.com/2007/12/30/business/30digi.html>

¹⁰ Convention for the Protection of Human Rights and Fundamental Freedoms, Nov 4, 1950, 213 UNTS 222 (entered into force Sept. 3, 1953), Article 8

¹¹ Gabriela Zanfir, Tracing the Right to Be Forgotten in the Short History of Data Protection Law: The "New Clothes" of an Old Right. in Gutwirth and others (eds), *Reforming European Data Protection Law* (Dordrecht: Springer Netherlands 2015) 234

¹² European Convention on Human Rights, Article 10

contradiction to the freedom of expression¹³. However, similarly to other cases involving a conflict between two rights, the prevalence of either of the two is to be assessed on a case-by-case basis, with the help of a balancing test. Even where objective factors lead to the conclusion that the right to be forgotten should be upheld, such an action, although justified, still represents a restriction on the freedom of expression – a fundamental right, the recognition of which is of utmost importance in a modern, democratic society.

A second disadvantage of the GDPR provision is the misleading nature of its wording¹⁴. In particular, the word ‘forgotten’ leaves the data subject with the impression that any information regarding them which has surfaced online can be taken down without any trace – in other words, forgotten. This, however, is not the case. The right to erasure, which has previously existed in the Data Protection Directive, still holds a number of requirements to be fulfilled in order for a piece of information to qualify for deletion. The word ‘forgotten’ exists nowhere in the provision itself, except for its title. Its impact, however, is colossal as it provides a false impression that any information can indeed be immediately destroyed, leaving no trace behind.

Furthermore, the right to be forgotten cannot act retroactively¹⁵. To expand on that, the damage already caused by the disclosure of certain information cannot be reverted. Although personal data can be erased on the basis of Article 17 GDPR, chances are that this data has already had an impact of a kind. To give an example, in the case of Stacy Snyder, even if the disputed picture had been taken down before the supervisors at the educational institution have had the ability to come across it, it has already been seen by a large number of other people. Moreover, it is physically impossible for this image to be deleted from the memory of all those other individuals the same way it can be taken down from the Internet. Therefore, exercising the right to be forgotten and erasing certain information does not guarantee the data subject that this information won’t have a negative impact nonetheless.

Rationally, the right to be forgotten is used mostly for deletion of old and no longer relevant information. Due to the exponentially growing amount of data on the Internet, it follows logically that such outdated information as a data subject might want to have erased,

¹³ General Data Protection Regulation, Article 17(3)(a)

¹⁴ Christiana Markou, The ‘Right to Be Forgotten’: 10 Reasons Why It Should Be Forgotten. in Gutwirth and others (eds), *Reforming European Data Protection Law* (Dordrecht: Springer Netherlands 2015) 215

¹⁵ *Ibid* 217

would be buried deep down in a particular website anyway¹⁶. Furthermore, the older a specific piece of information gets, the more difficult it becomes to find. This sequence of events stultifies the purpose of the right to be forgotten – it is highly probable that an individual would not prefer to follow all the proceedings to have their personal data erased if it is already challenging for this data to be discovered.

In addition, the newly established right to erasure proves to be too demanding in two aspects. First, its scope covers control over too broad a network of websites, including not only primary sources of information, but also search engines directing towards those primary sources. The fact that the European Union puts primary sources and search engines under a common denominator for the purposes of data protection becomes apparent in the decision of the European Court of Justice in Case C-131/12 *Google Spain*, where the court concluded that since a search engine “‘collects’ [and] subsequently ‘retrieves’, ‘records’ and ‘organises’ within the framework of its indexing programmes, ‘stores’ on its servers and [...] ‘discloses’ and ‘makes available’” specific data, it should be considered a processor for the purposes of the Data Protection Directive¹⁷. This additional inclusion is to a certain extent pointless – if particular information is taken down from a website, there would be nothing left for the search engine to point towards anyway. Therefore, it is needless for those servers to be held responsible together with the primary sources. Second, the obligation required in Paragraph 2 of Article 17 GDPR on the side of the controller to ‘take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data’ is a task, the fulfilment of which is exceptionally challenging. As already mentioned above, distribution of information online occurs at a truly high pace which results in a great challenge for the primary source of the data at hand to trace all the controllers who have duplicated it and warn them about the data subject’s request. Although the wording of the provision implies a certain degree of leniency (the controller is only obliged to take reasonable steps and not to mandatorily fulfil the task), this obligation is nonetheless excessively burdensome. What is more, under the GDPR, it is only the primary source of the information that is under an obligation to have this information disposed of¹⁸. Since third parties who have

¹⁶ Ibid 218

¹⁷ Case C-131/12 *Google Spain and Google* [2014] ECLI:EU:C:2014:317 28

¹⁸ ‘Right to Be Forgotten’: 10 Reasons Why It Should Be Forgotten 206

duplicated it are not obliged to erasure, the fulfilment of the data subject's wish might prove to be much more hardly achievable than it initially seems.

The introduction of the right to be forgotten in the General Data Protection Regulation was met with great enthusiasm and many controversial opinions. After a brief analysis, however, one can reasonably reach the conclusion that the right does not offer much more than the previously existing in the Data Protection Directive right to erasure; it is the formulation of the title of the new provision that creates the illusion for a great leap forward in the sphere of privacy protection. The elimination of the requirement for incompleteness or inaccuracy of the data broadens the scope of the right which results in both positive and negative consequences for the data subject. It seems, however, that the disadvantages outweigh the benefits and thus, this essay concludes that the right to be forgotten is a redundancy more than a necessity in the context of cyberspace.

Bibliography

Primary sources

- Convention for the Protection of Human Rights and Fundamental Freedoms, Nov 4, 1950, 213 UNTS 222 (entered into force Sept. 3, 1953)
- 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) [2016] OJ L119/1
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31
- Case C-131/12 *Google Spain and Google* [2014] ECLI:EU:C:2014:317

Secondary sources

- Cesare Bartolini and Lawrence Siry, 'The right to be forgotten in the light of the consent of the data subject'[2016] 32(2) Computer Law and Security Review
- Christiana Markou, The 'Right to Be Forgotten': 10 Reasons Why It Should Be Forgotten. in Gutwirth and others (eds), *Reforming European Data Protection Law* (Dordrecht: Springer Netherlands 2015)
- Gabriela Zafir, Tracing the Right to Be Forgotten in the Short History of Data Protection Law: The "New Clothes" of an Old Right. in Gutwirth and others (eds), *Reforming European Data Protection Law* (Dordrecht: Springer Netherlands 2015)
- 'Internet Usage Statistics' Internet World Stats, Miniwatts Marketing Group, 30 June 2018 <www.internetworldstats.com/stats.htm>
- Randall Stross, 'How to Lose Your Job on Your Own Time' The New York Times, 30 December 2007 <www.nytimes.com/2007/12/30/business/30digi.html>