Prof. Avv. Oreste Pollicino – oreste.pollicino@unibocconi.it

Avv. Marco Bassini – marco.bassini@unibocconi.it

We have been asked to advice, by the present opinion, on the legal and economic impact of the implementation of the Right of Reply (hereinafter, "RoR") platform with a view to facilitating the enforcement of the right to a proper representation of the identity of legal and natural persons on the Internet.

EXECUTIVE SUMMARY

- The right to be forgotten (or right to delisting) constitutes an expectation finding its roots in EU law as well as in the domestic legal orders of Member States, as per the Court of Justice of European Union interpretation in the *Google Spain* case. Such right is inherently in tension with freedom of expression, i.e. with the right to freely impart and receive ideas, opinion and thoughts.
- The advent of the Internet has resulted in the flourishing of unprecedented legal issues affecting, on one hand, the creation and dissemination of information by qualified and non-qualified operators, on the other one, the protection of individuals' reputation. While the Internet is creating new and more opportunities for media outlets and consumers, digital technologies are also negatively affecting the sphere of personal identity.
- A first problem lies with the circulation of dated and no longer updated news. The simple passing of time makes information that was correct at the time of the publication no longer accurate. The passing of time does not make *per se* false the piece of information at issue. However, it represents a scenario and conveys a message that is not entirely matching the reality, because of some developments occurred thereafter.
- Another problem concerns the spread of non-reliable information, false information, hoaxes or so called "fake news": content that does not constitute the product of the proper exercise of the freedom of information.
- Protection of reputation online is one of the most pressing needs of legal and natural persons. The advent of the Internet and of the new technologies has made it harder and harder for individuals to keep control of their personal identity as they used to do in the real life.
- Balancing freedom of information, on one hand, and data protection as well as personal reputation, on the other one, may turn out to be very difficult under

certain circumstances: the *Google Spain* judgment did not offer any specific criteria for the relevant operators to handle the delisting. Also, this implies significant efforts in terms of resources to be employed by search engine providers.

- Search engine providers would prefer to leave publishers and legal/natural persons free to determine the appropriate arrangements to apply without any direct interference in search results. In fact, the business model of Internet service providers is based on the assumption that these operators are merely neutral and passive and have no control over contents or information posted by third parties, such as websites' owners and publishers.
- The *Google Spain* case has brought to light the existence of a broad demand for protection of the individuals' reputation on the Internet. It also contributed to spread the awareness among the general public about the existence of a legitimate expectation to have certain information delisted when it no longer reflects the personal identity in an accurate way. The right of reply may come into play in at least two circumstances.
- First, the right of reply is recognized by some legal orders as the right of everyone to defend himself/herself against criticism, generally in the same form or venue where the relevant allegations were published. The right of reply does not have any specific constitutional ground, neither at supranational level nor at domestic one; however, it seems to find its roots in the interest to protect one's personal identity. In some legal orders, e.g. in Italy, the right of reply is guaranteed at legislative level in the specific context of press defamation. More precisely, the prerequisite of the right of reply consists in the prior publication of either images or statements/thoughts/acts referred to a natural/legal person which, in the view of the applicant, are harmful to his/her dignity or false
- In this respect, it should be questioned whether the implementation of the Right of Reply platform by the publisher would constitute a sufficient ground to consider the right of reply of the relevant legal or natural persons appropriately protected and thus exclude liability for publishers in connection to the failure to publish a reply on their website.
- Important benefits are more likely to occur in the context of the enforcement of the right to data protection, in particular to the extent the right of reply may work as an alternative to the delisting of content from the results generated by search engines.
- The *Google Spain* case has raised some concerns, particularly in light of the significant impact that the handling of individuals' requests may have on the freedom to conduct business of search engines. Additionally, chilling effects for the

right of publishers to impart information and the right of consumers to access to the same may derive from the implementation of the delisting procedure.

- Under Article 16 of the GDPR, "*The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement*".
- Upon certain circumstances, then, the protection of personal data may not require the removal of links from search results; rather, inaccurate or incomplete personal data can be subject to rectification.
- The shift from the right to rectification to the right to erasure can be regarded as a matter of degree: when information is still of public interest and the conditions for the removal of the same are not met, the rectification turns out to be the last resort for individuals to make sure that their data on the Internet accurately reflect the personal identity. In this scenario, the exercise of the right of reply does not depend on the existence of defamatory contents or contents which in any way harm personal dignity. Rather, the rectification is based on the processing of personal data that are no longer accurate or complete.
- The Right of Reply platform seems to be more likely appealing to both publishers and individuals when the enforcement of the right to data protection is at issue. In fact, Article 19 of the GDPR provides that the controller must take the necessary steps to inform the recipients of personal data of the rectification or erasure of the same. This obligation may be difficult to fulfill, since each publisher is supposed to disclose publicly information.
- Even if there is no way to require search engine providers to specifically implement the Right of Reply platform, the latter may definitely serve the purpose of notice any third party of the rectification of the concerned personal data. This option may reduce costs for both publishers and search engines.
- The best scenario to measure the effectiveness of Right of Reply as a possible tool for rectifying data and noticing third parties the rectification thereof would be to build up a *casus belli* to obtain a decision of the competent administrative/judicial authority validating or not the implementation of the platform as a solution that may permit the relevant parties to comply with the law. Nonetheless, the solution offered by Right of Reply is promising, also in light of some developments in the relevant case law.
- In any case, it has to be stressed that, also in light of the protection of the freedom to conduct business, there is no legal basis for imposing the adoption of the Right of Reply platform on search engine providers. They can definitely

implement the interface offered by Right of Reply on a voluntary basis, as part of their business.

- Other elements should be taken into account while assessing the actual degree of compatibility of the Right of Reply platform with the legal and regulatory framework.
- Some concerns may arise in connection with the notion of editorial responsibility. Internet service providers, including search engine providers, do not exercise any editorial control over the content posted by third parties. Accordingly, they are subject to liability exemptions on the assumption that the service provided is of merely automatic, passive and neutral nature. It is largely debated among scholars and courts whether certain activities that are commonly performed by providers call into question the automatic, neutral and passive nature of the relevant service and, accordingly, the applicability of the liability exemptions for any illegal content. Recently, the debate has come up with respect to the contrast to the spread news and possible implementation of algorithms or fact-checking mechanisms relying on third parties' services. The adoption of these measures is deemed to create room for an exercise of editorial responsibility that might deprive service providers of the liability exemptions.
- From a general and policy perspective, the goal of Right of Reply is to create more debate and more room for ideas, opinions and thoughts to be exchanged on the Internet. From this standpoint, the business strategy of Right of Reply is definitely compatible also with the view, already endorsed by the US Supreme Court, that the Internet enhances the free marketplace of ideas.
- Article 4 of the E-Commerce Directive also stipulates that '*Member States shall ensure that the taking up and pursuit of the activity of an information society service provider may not be made subject to prior authorization or any other requirement having equivalent effect*'.
- In light of these provisions, if the service provided by Right of Reply meets the requirements outlined in the definition of Information Society service ("*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*"), it may enjoy the regime excluding any prior authorization or requirement having equivalent effect.
- However, given the absence of speculation or case law on the nature of services similar or comparable to those offered by Right of Reply, it cannot be excluded at all that courts or regulatory authorities might require it to comply with certain requirements on the basis of the existence of a degree of editorial control over content.

The following assessment moves from the background illustrated in the opinions by Mr. Rosboch and Ms. Paruzzo. In particular, it assumes that the right to be forgotten (or right to delisting) constitutes an expectation finding its roots in EU law as well as in the domestic legal orders of Member States, as per the Court of Justice of European Union (the "Court of Justice") interpretation in the *Google Spain* case[1]. The right to be forgotten / right to delisting, more precisely, derives its status as constitutional right from the provisions enshrined to Article 7 and 8 of the Charter of Fundamental Rights of the European Union ("Charter") which establish, respectively, the right to private life and the right to data protection. Also, it is part of the right to private and family life under Article 8 of the European Convention on Human Rights ("ECHR"). As such, the right to be forgotten / right to delisting is inherently in tension with freedom of expression, i.e. with the right to freely impart and receive ideas, opinion and thoughts, protected by Article 11 of the Charter and Article 10 ECHR.

The assessment will explore the legal and economic challenges that may arise in connection to the implementation of the RoR platform, on the basis of the legal status of the right of reply in the domestic and European legal order. In particular, the first parts of the opinion will focus on whether the service provided by RoR may fit with the existing legal background in respect of the enforcement of the right of reply *stricto sensu* in the specific context of defamation and as a possible means for rectification under the relevant data protection framework. In the second part, the opinion will address the legal qualification of the service, with a view to determining whether the same may be subject to specific authorizations or requirements by Member States.

***

Right of Reply LTD aims at developing and marketing a unique service and solution to the issue of protection of personal rights in the context of search

[1] Court of Justice of the European Union, Case C-131/12.

engines and social networks. It is an applied patent technology related to the assertion of personal rights. RoR is a pay by subscription service, system and technology which provides a rapid, effective and legal solution to a particular problem, i.e. the protection of one's reputation, by preventing the negative effects occurring when a natural/legal person becomes the target of various content spread over the Internet, in the form of articles, images, videos, blog comments, etc. The concerned persons have historically found that it is difficult, if not practically impossible, to respond to and/or obtain redress for attacks on one's identity.

Defending one's personal reputation is undeniably time-consuming and costly, with the burden on the affected person to substantiate his/her claim before the relevant authorities.

RoR, through a series of proprietary registered patented technology and applications, has developed a simple, effective, inexpensive solution which:

1) enables the RoR subscriber using a personal RoR page to:
    a. be informed of any web content (including but not limited to articles, images, videos, blogs, forums or the like which mentions or quotes them in any way), through the "All About Me" tool;
    b. have all such content available on a page that is promptly and automatically updated;
    c. make use of the patented "Check The Text" tool which runs a proprietary algorithm which analyzes content using the following parameters: (i.) content circulation, (ii.) content accuracy, (iii.) damage assessment, (iv.) most used word cloud. As a result, subscribers can obtain at a single glance an unbiased and objective evaluation of the web content that affects them;
    d. have the ability to respond to negative content by submitting a reply in the same web content with a personal version of the facts

behind the negative post, be it an article, image, video, blog, forum etc., through the "My Truth" tool;

e. set up a web content review which enables subscribers not only to receive every piece of content which concerns them but also to immediately respond whenever and wherever necessary, and thereby have the ability to contextualize that content with their own version of the facts;

f. make available all the web content which relates to them along with their own comments through the specific RoR social network;

g. place at the disposal of every possible RoR search engine user not only all of the content available on the web which concerns them, but also their own replies to that same content;

h. access every other search engine, through the patented "Response Availability Asterisk" tool, to advise viewers of a specific item of web content that the subscriber's own response to the content which has been accessed by the viewer is also available. In this manner, next to every link on the web which contains a negative matter there will be a RoR asterisk which signals to anyone accessing such negative matter that there is also a response from the person mentioned in the content available on that URL;

i. the ability, through the patented "Announce It To All" tool, to alert anyone who in the past has viewed the content, that a response has been provided by the person subject of the specific content that they have viewed;

2) enables the RoR web user searching a person on RoR page to:

a. use the RoR search engine to find all of the content available on the web concerning a specific person;

b. obtain a rapid, unbiased and impartial analysis of the nature of an item of web content in order to be able to access it with objectivity and clarity;
c. be able to know and read from a single page not only everything that is available on the web concerning a specific person, but also to view that same person's specific replies, comments, opinions or version of the facts regarding the same content;
d. know whether a link found on another search engine regarding a specific person is supplemented by a response from that same person, through the featuring of a Response Availability Asterisk;
e. be notified whenever a response to a piece of content viewed in the past on RoR becomes available, through an Announce It To All tag;

3) enables the search engines that facilitates the use of RoR to:
a. provide a useful additional service for their users;
b. be able to guarantee important rights such as the right to respond, the right to privacy, the right to plurality of information, the right of expression, by enabling the presence of RoR tools, banners and responses on their search engines;
c. avoid being the target of legal action, or various types of claim, on the part of those who feel they have been damaged by the fact that search engines provide access to every type of content, even though they are not responsible for the content;
d. be able to guarantee the rights of everyone, and accordingly to actively safeguard their reputation;
e. improve their reputation along with their users' perception of the social responsibility of the search engine, and thereby to improve their own social image;

4) enables society in general to:
    a. see fundamental rights exercised and protected, such as the right to personal identity, the right to freedom of expression, the respect of one's personal image, the right to privacy in its sense as the right to truthfulness;
    b. see the implementation of an effective balance between the collective right to know and the individual right to let the truth be known;
    c. see fulfillment of the right of access to information, which can only be attained through a plurality of sources through which knowledge is gained, so that people are free to form opinions based on several points of view.

***

LEGAL AND ECONOMIC ASSESSMENT

Introduction: the conflict between freedom of expression and the right to one's personal identity

The service provided by RoR impacts a very critical relationship, most notably after the rise of the new digital technologies: namely, that between publishers and individuals who may experience harmful consequences deriving from the circulation of non-accurate, non-reliable or non-updated information.

The advent of the Internet has resulted in the flourishing of unprecedented legal issues affecting, on one hand, the creation and dissemination of information by qualified and non-qualified operators (including professional newspapers and journalists, blogs, forum), on the other one, the protection of individuals' reputation. While the Internet is creating new and more opportunities for media outlets and consumers, since a new channel is now available to impart or seek information *in real time*, digital technologies are also negatively affecting the sphere of personal identity. Some challenges derive, particularly, from the

unrestricted flow of information to which the World Wide Web has given rise. In this respect, it is of utmost importance to take the role of search engine providers into account. The indexing of contents retrieved from third parties/publishers' websites makes it much easier for natural and legal persons to find information relating to specific individuals. However, this scenario may raise some concerns when it comes to dated information or inaccurate information that is nevertheless available on the Internet without any filter or specific measure that may discriminate information based on the respective timing.

Natural and legal persons, whose reputation is at hand, may therefore experience at least two different problems.

The first problem lies with the circulation of dated and no longer updated news. In this scenario, the simple passing of time makes information that was correct at the time of the publication no longer accurate. The passing of time does not make *per se* false the piece of information at issue. However, it represents a scenario and conveys a message that is not entirely matching the reality, because of some developments occurred thereafter. Even though the information that becomes inaccurate is not illegal, its circulation as such may nevertheless affect the reputation of the relevant natural or legal person. As it is well known, the Court of Justice has taken some important steps in this regard in the *Google Spain* decision, also urging national data protection authorities to take this judgment into account. More recently, the General Data Protection Regulation (EU Regulation no. 2016/679, also "GDPR"), which be directly applicable after May 25, has expressly provided for the right to be forgotten as one of the rights of the data subject.

It is worth noting that the implementation of the *Google Spain* judgment may result in a black-white decision: to remove or not links to inaccurate/non update content from the search results generated through the use of a certain keyword. The publisher's website containing inaccurate or non-update information is not subject to any editorial intervention, since it is only excluded

from the indexing from the algorithms. However, individuals as well as legal persons may also have an interest to have certain information updated in the website that is the source of the same. Newspapers would face significant costs if they were required to update over the time the news once the same have been published and certain time has passed. Such an activity (that the Italian Supreme Court required to implement in judgment no. 5525/2012) would be time-consuming for newspapers and journalists. However, an option to notice the relevant developments could be to allow the concerned legal/natural persons to "reply", requiring the insertion of a reference to the event occurred thereafter. This way, no matter whether the news would be subject to indexing by search engines or not, the content of the website could be kept posted over the time upon request of the concerned person.

The second problem concerns the spread of non-reliable information, false information, hoaxes or so called "fake news": in a nutshell, content that does not constitute the product of the proper exercise of the freedom of information. The scope of the present analysis will be limited to the circulation of defamatory or non-accurate content, in connection to which legal orders are generally providing individuals with a right of reply with a view to limiting the relevant harmful effects. However, policymakers and courts are currently facing similar challenges raised the spread of disinformation and hate speech, that may be based on the use made with intent of defamatory content. Recently, the High Level Expert Group on Fake News and Online Disinformation released its final report, where it is said that disinformation is a phenomenon going beyond the term "fake news". Disinformation includes "all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit". Instead, it does not cover issues arising from the creation and dissemination online of illegal content (including, e.g., defamation, hate speech, incitement to violence), which are subject to regulatory remedies under EU or national laws, nor other forms of deliberate but not misleading distortions of facts

such a satire and parody. Accordingly, fight against disinformation is topical in the legal and economic debate and new business models such as that of RoR may definitely leverage on the ongoing stances at legislative and regulatory level.

Furthermore, the rise of the Internet has resulted in the dramatic drop of the costs for producing information and the emergence of citizen journalism. Everyone is nowadays capable, without incurring significant expenses, of creating a blog or a news portal and gaining even significant reach and interactions on social media; this way competing, ultimately, with professional newspapers and journalists. Among non-qualified sources of information, non-reliable websites and portals may even be *prima facie* recognized as such when users access their websites, however search engines cannot be prevented from retrieving and indexing the content of the same. Also, contents spread through these platforms are more likely to become "viral", and thus subject to massive sharing by users.

Finally, in addition to the spread of fake news and of non-professional information platforms, defamation may definitely occur also in the context of professional journalism. Press defamation indeed is still a quite serious problem. Most notably, public figures may trigger defamation complaints to make pressure on media while reputation of any individual may be significantly impacted. The more information is quickly spread on the Internet, the more likely it may be inaccurate.

This scenario is relevant also from an economic standpoint. The rise of the Internet has resulted in unprecedented changes affecting the market of media. As noted in the report released by Berkeley Economic Advising and Research (BEAR), one of the consequences of the digital revolution lies with the decentralization of the supply side of media information flows by virtue of the growth of Internet access and the reduction of transaction costs. The development of the Internet has thus led to the creation of new opportunities, most notably in light of the high

penetration of social media.[2] Coupled with the growth of social media is a rising skepticism of users on credibility and reliability of information: the Internet is less trusted than broadcast and print media. As the BEAR report specifies, lower degrees of Internet trust are common to states with higher incomes and education levels. Thus, quite paradoxically, online media are at once the least trusted and most popular information resources. Everyone is more and more connected but also more vulnerable. This may result in creating more grounds for a successful implementation of a business model such as RoR to identify and remedy misinformation in a new market of digital reputation and credibility management. From an economic standpoint, fake news have negative reputational effects, raising direct and indirect costs for natural and legal persons.

The implementation of the right to delisting and the relevant legal challenges

In light of the foregoing, protection of reputation online is one of the most pressing needs of legal and natural persons. The advent of the Internet and of the new technologies has made it harder and harder for individuals to keep control of their personal identity as they used to do in the real life (world of atoms). A new concept, namely that of digital identity, has emerge in case law and academic speculations. Accordingly, protecting personal identity becomes even more difficult in the age of the Internet, because of the fragmented nature of the data concerning the same (legal/natural) person that may be disseminated throughout the World Wide Web.

Balancing freedom of information, on one hand, and data protection as well as personal reputation, on the other one, may turn out to be very difficult under certain circumstances. With respect to information that is no longer of

[2] The BEAR Report *Right of Reply –Tell your Truth* estimates that if RoR marketing were restricted to the EU28, it would cover 500 million current social media subscribers, while in the Americas additional 600 million users can be targeted. Also, it reports that in 2017 nearly 3 billion users were active on social media, covering 37% of population.

public interest and that, as such, is subject to removal from the results generated by search engines, the *Google Spain* judgment did not offer any specific criteria for the relevant operators to handle the delisting. This way, private operators such as Google were *de facto* vested with a "quasi-constitutional task", i.e. balancing the different interests at stake. Particularly, determining which contents are of public interest may be tricky, also depending on the specific circumstances of the case. The decision to delist certain contents entirely rests in the hands of private operators, which are by default business oriented[3]. However, delisting content from search engines may, even to a certain degree only, affect the right of individuals to access information and that of publishers to impart information. Also, implementing the right to delisting requires significant efforts in terms of resources to be made by search engine providers. This holds even truer in light of the possibility for data subjects to challenge the decision to delist/not delist before the competent administrative or judicial authority. The burden on Internet service providers may therefore be significant, given the extreme uncertainty surrounding the criteria on which the delisting grounds. It is worth noting that the Charter of Fundamental Rights of the European Union expressly protects the freedom to conduct business under Article 16. In its previous case law, and namely in the *Scarlet v. Sabam* (2011)[4] and *Sabam v. Netlog* (2012)[5] decisions, the Court of Justice took specifically into account the impact that implementing certain measures may have on freedom to conduct business with respect to the prevention of copyright infringements. The *Google Spain* case came therefore with some surprise, to the extent private actors are now actively involved in the removal of link (even though no obligation to monitor applies to them, as opposed to the providers at hand in mentioned cases) to certain contents. It can be argued, then, that search engine providers would definitely prefer to leave

[3] On the contrary, the solution provided by the RoR platform aims at protecting reputation of legal and natural persons through an independent credibility technology.
[4] Court of Justice of the European Union, Case 70/10.
[5] Court of Justice of the European Union, Case 360/10.

publishers and legal/natural persons free to determine the appropriate arrangements to apply without any direct interference in search results. It is worth noting that the business model of Internet service providers is based on the assumption that these operators are merely neutral and passive and have no control over contents or information posted by third parties. Accordingly, they do not exercise any editorial responsibility vis-à-vis the latter. However, the more Internet service providers are required to take some steps such as the removal of search results, albeit upon request of the relevant party, the more this assumption is called into question and they face the risk of exercising a degree of editorial control.

With respect to defamatory contents, even more complicated problems may arise. In this scenario, allegedly illegal contents are at stake. As far as search engine providers are concerned, Directive 2000/31/EC (the "E-Commerce Directive") establishes that they have no responsibility for the automatic, intermediary and temporary storage of information, among others, when "*the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement*". Accordingly, they are not supposed to take any specific step where the above conditions are not met. However, this may weaken the protection of legal or natural persons who claim to have been defamed, since the removal from the search results comes into play only as result of a specific procedure, implying an assessment of the defamatory nature of the content that may take significant time. Also, once the competent authority has ascertained the defamatory nature of contents or information, this would not necessarily trigger the removal of the same. Since the contents would possibly remain available on both the website/source and the search engine, the concerned persons may have an interest in reducing the impact of the circulation of said contents. Even in the

case the website that is the source of defamatory content hosts a reply by the concerned persons, the latter is unlikely to benefit from the same degree of circulation that the original content enjoyed when it was first published. As a consequence, news or content having a significant negative impact on individual or business reputation may still be available among the search engines' results, so that protecting one's reputation may turn out to be difficult even if the legal remedies are actually enforced.

As noted above, the scope of this opinion does not extend to the role of caching providers, namely search engine service providers. Nevertheless, the difficulties raised by the involvement in the takedown procedure of parties other than publishers and persons should be taken into account to assess the actual degree of protection that the latter may expect when enforcing the existing legal remedies and regardless of the specific legal order.

The *Google Spain* case has brought to light the existence of a broad demand for protection of the individuals' reputation on the Internet. It also contributed to spread the awareness among the general public about the existence of a legitimate expectation to have certain information delisted when it no longer reflects the personal identity in an accurate way. It is then of utmost importance considering the pressure that natural and legal persons may exercise while seeking protection in this respect. This trend is also showed by the most recent legislative developments, in particular in the new Article 17 of the GDPR, which protects the "right to erasure" / "right to be forgotten". This provision captures the importance of considering not only the relationship between data subjects and data controllers (i.e. individuals and publishers) but also that between the data controllers and any third party processing the personal data of the data subject where the same have been made public (i.e. publishers and search engines). Statistics show how search engines have become one of the main sources of information for consumers. The 2017 report on the consumption of information released by the Italian Communication Authority (AGCOM), for

instance, notices that 54.5% of the population uses algorithmic sources (including social media and search engines), and that 36.5% of this quota regard search engines as the first source of information. A global poll launched by Google in 2014 reported that 91% of online adults use search engines to find information on the web, while 65% of people see search as the most trusted source of information on legal and natural persons. Also, individuals are aware of the problem of spreading disinformation and the existence of many non-reliable sources of information. Search engines may therefore have a very important impact on reputation. It is not by chance that the possible initiatives discussed by policymakers and stakeholders with a view to contrasting fake news include the use of special graphic features to notice users that certain news or information has been fact-checked. When information is retrieved in publishers' website, through an internal search engine, users may more easily notice that the relevant news was published in the past and that some developments may have occurred as result of the passing of time. The problem, then, mainly occurs when users look for certain information on search engines such as Google and Bing. It is in this specific context that data subjects may claim to update the existing information and news or to notice that the same do not appropriately represent the individuals' reputation or identity.

The constitutional relevance of the right of reply

From a legal perspective, the right of reply may come into play in at least two circumstances.

1. First and foremost, the right of reply is recognized by some legal orders as the right of everyone to defend himself/herself against criticism, generally in the same form or venue where the relevant allegations were published. The right of reply does not have any specific constitutional ground, neither at supranational level nor at domestic one; however, it seems to find its

roots in the interest to protect one's personal identity. In some legal orders, e.g. in Italy, the right of reply is guaranteed at legislative level in the specific context of press defamation. More precisely, the prerequisite of the right of reply consists in the prior publication of either images or statements/thoughts/acts referred to a natural/legal person which, in the view of the applicant, are harmful to his/her dignity or false. Failure to comply with the obligation to publish a reply may result in a fine ranging from Euro 1,500.00 to 2,500.00. In Italy, according to a trend of case law, the right to respond granted by the Law 47/1948 is not applicable to the online versions of the newspaper. However, there is room to maintain that such right shall be granted also for online publications and to claim that, as in the case of print media, newspapers can be obliged to publish the reply.

In addition to the above, Article 8 of Law 47/1948 provides that the reply must be published at the top of the same page where the article to which the reply refers was placed. Also, the reply must have the same visual characteristics as the article to which it refers. This provision was framed with a view to regulating printed media, since the Internet did not yet exist at that time. In light of the rationale behind this provision (attaching the reply equal emphasis as the original publication), it can be debated whether said requirements may be met by inserting a link to the reply or embedding the reply itself into the same webpage where the article was posted. Likewise, it can be disputed whether the use of a platform having the specific characteristics of RoR would allow publishers to fulfill their obligations (if any).

It is worth noting that the publication of the reply does not exclude *per se* liability for defamation. For instance, in Italy, the Supreme Court expressly pointed out that publishing a reply does not remove the harmful consequences of a defamatory conduct, but only reduces the impact thereof. Accordingly, it may be taken into account, e.g., when determining

the amount of the damages to be awarded to the person who was harmed by the defamatory content.

Regardless of the specific context of the Italian legislation, it should be questioned whether the implementation of the RoR platform by the publisher would constitute a sufficient ground to consider the right of reply of the relevant legal or natural persons appropriately protected and thus exclude liability for publishers in connection to the failure to publish a reply on their website.

However, against this background, it should be explored if search engines would obtain any benefits from the implementation of the RoR platform and, most notably, how they can be required to do so. In this respect, it seems difficult to outline specific legal advantages that search engines may derive from the implementation of a mechanism such as that provided by RoR.

2. Important benefits are more likely to occur in the context of the enforcement of the right to data protection, in particular to the extent the right of reply may work as an alternative to the delisting of content from the results generated by search engines.

As noted above, in the *Google Spain* case the Court of Justice ruled that data subjects are entitled, under certain conditions, to ask search engines for the removal of pieces of information that are no longer accurate, mainly because of the passing of time.

This judgment has raised some concerns, particularly in light of the significant impact that the handling of individuals' requests may have on the freedom to conduct business of search engines. Additionally, chilling effects for the right of publishers to impart information and the right of consumers to access to the same may derive from the implementation of the delisting procedure.

It is also worth considering that most of the requests submitted by legal and natural persons to get their personal data removed from search results are rejected. In light of these factors, individuals may probably find a better remedy in the right to rectification, under Article 16 of the GDPR. According to this provision, "*The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement*". It can be argued, thus, that under certain circumstances the protection of personal data may not require the removal of links from search results; rather, inaccurate or incomplete personal data can be subject to rectification. This may hold true especially in case the relevant news is still of public interest and therefore may very unlikely be delisted from the search results. In this scenario, data subjects may nevertheless have an interest to get the information relating to himself/herself updated and thus to enforce the right to rectification under Article 16 of the GDPR.

The shift from the right to rectification to the right to erasure can be regarded as a matter of degree: when information is still of public interest and the conditions for the removal of the same are not met, the rectification turns out to be the last resort for individuals to make sure that their data on the Internet accurately reflect the personal identity. In this scenario, the exercise of the right of reply does not depend on the existence of defamatory contents or contents which in any way harm personal dignity. Rather, the rectification is based on the processing of personal data that are no longer accurate or complete. However, the rationale behind the reply in these circumstances is not much different from that underlying the reply in the context of press defamation: in both cases, rectification serves to reduce the negative impact that online

information, whether defamatory or simply inaccurate/incomplete, may have on the reputation of legal and natural persons.

From an economic standpoint, it is worth noting, as pointed out in the BEAR report, that there has been a shifting from punitive defamation and libel actions toward privacy defense in the reputational defense area. According to a Reuters survey, a privacy claim for inaccuracy of information is more effective than libel. This scenario fits very well with the RoR platform, which seems to have potential for discouraging defamation or libel claims, most notably when it comes to information that is merely inaccurate, dated or non-updated. Also, whatever claim (either defamation or privacy) is raised, legal recourse against disinformation is quite inefficient, since these remedies are slow and expensive if compared to the degree of complexity of Internet and digital technologies. This way, the RoR platform can definitely pave the way to a new generation of credibility technologies based on a new model of "dialog news" (as noted in the BEAR report).

Focus: the right of reply as alternative to the erasure of personal data

When it comes to rectification of inaccurate or incomplete personal data, the RoR platform seems to be more likely appealing to both publishers and individuals. In fact, Article 19 reads as follows: "*The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it*".

This provision establishes that the controller must take the necessary steps to inform the recipients of personal data of the rectification or erasure of the same. This obligation may be difficult to fulfill, since each publisher is supposed to

disclose publicly information. The purpose of this provision is to make sure that the activities carried out by search engines, among others, do not deprive data subjects of the benefits deriving from the rectification or erasure of data. In this respect, even if there is no way to require search engine providers to specifically implement the RoR platform, the latter may definitely serve the purpose of notice any third party of the rectification of the concerned personal data. This option may reduce costs for both publishers and search engines. The former can argue that their obligation to inform the recipients to whom personal data have been disclosed that the same have been subject to rectification is fulfilled by reason of the existence of a mechanism such as that underlying the RoR platform. The latter are relieved from a time-consuming activity such as handling individuals' requests to delist certain search results. Ultimately, this option, by encouraging rectification instead of erasure, seems to be more desirable from a public policy perspective, to the extent it limits chilling effects on freedom of expression and fosters a more balanced approach to reconcile freedom of information (both the impart and to receive the same) and protection of personal data.

As suggested by Mr. Rosboch in his opinion, the best scenario to measure the effectiveness of RoR as a possible tool for rectifying data and noticing third parties the rectification thereof would be to build up a *casus belli* to obtain a decision of the competent administrative/judicial authority validating or not the implementation of RoR as a solution that may permit the relevant parties to comply with the law. Prior to such possible decision, assessing the "legal fitness" of the RoR platform would be possible only *in abstracto*. Nonetheless, the solution offered by RoR is promising, also in light of some developments in the relevant case law.

It is worth noting that in the *Wegrynowski and Smolczewski v. Poland*[6] (2013) judgment the European Court of Human Rights held that the removal from the Internet of certain news would amount to a violation of Article 10 ECHR,

[6] European Court of Human Rights, App. 33846/07.

protecting, as we have outlined above, freedom of expression. The Court said, in a case concerning the publication in the digital version of news that had already be found defamatory at the time of the release of the paper version of a newspaper, that the rectification can be a sound solution to balance the protection of the applicants' reputation and the safeguarding of freedom of information. In order for both these interests to be guaranteed, the publication of a short notice or a link to further relevant information (in the case, to the court judgment finding the article to be defamatory) would be appropriate. The Court also stressed that the removal of an article from a newspaper, requiring an order of the judicial authority, would entrust judges with the role of historians, thus creating serious challenges for freedom of expression. Also, this measure would be disproportionate to the aim of protection the reputation of the applicants, since less restrictive mans, such as the rectification, exist and could be enforced vis-à-vis the publisher. Even though this case does not involve the delisting from search results (the removal of the article from the online version of the newspaper was at stake), it turns out to be telling with regard to the importance of rectification and, possibly, of the right of reply as a means to ensure protection of personal reputation without giving rise to chilling effects on freedom of information and to much broad room to search engines while determining to remove or not certain links from search results.

Such important value of rectification also came up in another landmark decision of the Italian Supreme Court (judgment no. 5525/2012). In this case the Italian Data Protection Authority first and courts later had to face the request of protecting the reputation of a former politician (thus, a public figure) who claimed that some news relating to him were no longer update to the extent they did not include the further developments of a criminal proceeding. The Supreme Court found that the removal of the news was not possible since the person was still a public figure and the information relating to him was still of public interest. However, the Court said that the applicant had a right to a correct representation

of his personal identity, which required the publisher to update the news by the insertion of all the relevant details concerning the facts occurred after the publication of the piece. This way, the news was said to be "contextualized". This decision raised some concerns among publishers, since it was supposed to introduce an obligation to monitor on a regular basis the content of news with a view to updating the content of the same. However, most of scholars who commented on this judgment noted that this obligation, based on the applicable data protection law in force in Italy (Italian Data Protection Code, Legislative Decree no. 196/2003), can be enforced only upon request of the party (i.e. the data subject). Accordingly, publishers are not required to monitor the content of news included in the relevant online archives, but only to contextualize some pieces of information once requested by the legal or natural person who claims that his/her/its reputation is harmed. Since this solution has been recognized by courts as viable for protecting the personal identity of legal and natural persons, the same result may likely be reached, from an empirical perspective, through the implementation of the RoR platform.

The references to the decision of the European Court of Human Rights and the case delivered by the Italian Supreme Court support the view that courts and data protection authorities are generally looking at the actual degree of protection of the data subject, regardless of the specific means through which this objective is fulfilled. Based on the description of its functioning, the implementation of the RoR platform might reasonably be ranked among the various means by which to obtain such result.

More recently, the Supreme Court (judgment no. 6919/2018) also pointed out, in an *obiter dictum*, that one of the conditions where the right to be forgotten can be limited for the sake of freedom of information lies with the existence of a prior notice given to the data subject concerning the publication or the broadcasting of dated news/content, to make it possible for the latter to exercise his/her right of reply.

Nonetheless, it has to be stressed that, also in light of the protection of the freedom to conduct business, there is no legal basis for imposing the adoption of the RoR platform on search engine providers. They can definitely implement the interface offered by RoR on a voluntary basis, as part of their business.

However, other elements should be taken into account while assessing the actual degree of compatibility of the RoR platform with the legal and regulatory framework.

Some concerns may arise in connection with the notion of editorial responsibility. It is commonly accepted that Internet service providers, including search engine providers, do not exercise any editorial control over the content posted by third parties (e.g., the publisher or the owner of a website). Accordingly, they are subject to liability exemptions on the assumption that the service provided is of merely automatic, passive and neutral nature. It is largely debated among scholars and courts whether certain activities that are commonly performed by providers (including categorizing contents or providing advertising messages) call into question the automatic, neutral and passive nature of the relevant service and, accordingly, the applicability of the liability exemptions for any illegal content. In Italy, for instance, some courts found that, where certain conditions are met, a service provider does no longer act in a merely automatic, passive and neutral way, as it is assumed to exercise a degree (albeit limited) of control over content. In this scenario, the so called *active* providers should be subject to the liability rules applicable to content providers. It is worth noting that this interpretation, even if accepted by some influential courts in Italy, has no specific grounds in the text of the relevant provisions (namely, the E-Commerce Directive and the national provisions which implemented it into the domestic legal order). However, Internet service providers could more likely face liability by reason of the implementation of additional tasks. Recently, the debate has come up with respect to the contrast to the spread news and possible implementation of algorithms or fact-checking mechanisms relying on third parties' services. The

adoption of these measures is deemed to create room for an exercise of editorial responsibility that might deprive service providers of the liability exemptions. Also in this respect, there is now specific legal basis to assert that these techniques exclude the merely automatic, passive and neutral nature of the service. However, it cannot be excluded, especially in light of the aforesaid trends in case law, that courts may take the view that the implementation of said measure amounts to an exercise of editorial responsibility, which would therefore shift from the publisher to the service provider. This scenario may discourage search engine providers to take any step that would allow natural and legal persons to interact with the content of publishers websites through the search results.

It is necessary to consider another critical factor that is inherently related to the cross-border nature of the Internet. After the *Google Spain* decision, some concerns grew out in the US, where most of the Internet companies are based. These concerns emerged as a reaction to the very specific understanding of the Court of Justice on the relationship between freedom of expression and data protection. It is not by chance that the delisting of search results is offered by Google and other search engines in the European Union, where the judgment of the Court of Justice is formally binding, but not in the US, where the broader protection of the freedom of speech supersedes that of personal data.

From a general and policy perspective, the goal of the RoR platform is to create more debate and more room for ideas, opinions and thoughts to be exchanged on the Internet. From this standpoint, the business strategy of RoR is definitely compatible with the view which the US Supreme Court endorsed starting from the *Reno v. ACLU* judgment that the Internet enhances the free marketplace of ideas. However, since the delisting of search results is felt as a less pressing social need than in Europe, this difference may have an impact on the decision of search engine providers to implement the RoR platform.

In addition to the foregoing, it is worth highlighting that the approach of the US Supreme Court in respect to the right of reply has been quite cautious. The

case law on the right of reply is not consistent. In *Red Lion Broadcasting v. FCC*[7] the Supreme Court upheld the regulations adopted by the FCC under the fairness doctrine, allowing for an attacked person to be given the right of reply within discussion of public issues. On the contrary, in *Miami Herald Publishing Co. v. Tornillo*[8] the Court overturned a Florida law which required print media to provide candidates for political offices who were assailed regarding their personal character or official record with the right of reply.

It is thus debated whether the right of reply is solidly grounded, most notably because of its possible spillover effects on freedom of press.

Authorization or equivalent requirements

Lastly, it has to be examined whether the operation of the service provided by RoR may be subject to any requirement or authorization. From a general perspective, there is no legislation at EU level regulating speech by imposing content-based restrictions. It is up to national lawmakers, thus, to carve out possible limitations on freedom of speech based on the safeguard of other compelling interests (e.g. reputation) in accordance with the three-prong test enshrined to Article 10 ECHR[9]. On the other hand, the activity performed by RoR may be relevant from the standpoint of free circulation of services. It is worth noting that Article 1 of Directive 2015/1535 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services defines the latter as " *any service normally provided*

[7] 395 U.S. 367 (1969)
[8] 418 U.S. 241 (1974).
[9] Namely, the limitations must be (i.) prescribed by law, (ii.) necessary in a democratic society and (iii.) pursuing legitimate aims, such as the national security, territorial integrity or public safety, the prevention of disorder or crime, the protection of health or morals, the protection of the reputation or rights of others, preventing the disclosure of information received in confidence, or maintaining the authority and impartiality of the judiciary.

for remuneration, at a distance, by electronic means and at the individual request of a recipient of services", whereas:

(i.) "*at a distance*" means that the service is provided without the parties being simultaneously present;

(ii) "*by electronic means*" means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;

(iii) "*at the individual request of a recipient of services*" means that the service is provided through the transmission of data on individual request.

Article 4 of the E-Commerce Directive also stipulates that '*Member States shall ensure that the taking up and pursuit of the activity of an information society service provider may not be made subject to prior authorization or any other requirement having equivalent effect*'.

In light of these provisions, if the service provided by RoR meets the requirements outlined in the definition of Information Society service, it may enjoy the regime excluding any prior authorization or requirement having equivalent effect.

Notwithstanding the above, given the absence of speculation or case law on the nature of services similar or comparable to those offered by RoR, it cannot be excluded at all that courts or regulatory authorities might oblige RoR to comply with certain requirements based on the existence of a degree of editorial control over content.

Milan, 16 April 2018

Prof. Avv. Oreste Pollicino Avv. Marco Bassini