LE DROIT À L'OUBLI EN EUROPE ET AU-DELÀ

THE RIGHT TO BE FORGOTTEN IN EUROPE AND BEYOND

Cet ouvrage interroge l'impact de l'arrêt *Google Spain c. Costeja*, quatre ans après son adoption. Il s'agit de comprendre comment ce droit à la nature ambiguë est mis en oeuvre par Google, mais aussi par les autorités de protection et les juridictions au sein d'Etats membres de l'UE. Cet ouvrage questionne également les futures évolutions du droit à l'oubli numérique en Europe notament avec l'arrivée prochaine du Règlement Général de la Protection des Données Personnelles (RGPD). Il invite à mieux saisir l'ancrage européen de ce droit en confrontant les solutions mises en place dans d'autres États principalement en Asie et en Amérique Latine pour répondre au besoin social de ne pas voir son histoire personnelle affichée de manière permanente sur Internet tout en protégeant la liberté d'expression. Enfin, cet ouvrage est le fruit d'une collaboration internationale initiée autour de la première e-conference organisée par blogdroiteuropéen en mai- juin 2017. Il rassemble des contributions de vingt chercheurs en droit et constitue le premier livre numérique de la collection Open Access Book de blogdroiteuropeen.

This book questions the impact of the *Google Spain v. Costeja* Case four years after its adoption. It analyses how this ambiguous right is implemented not only by Google, but also by data protection authorities and the judges in several European Member States. This book looks also at the future evolution of the European digital Right To Be Forgotten (RTBF) introduced in the General Data Protection Regulation, which will apply from 25 May 2018. This book allows understanding of the European anchorage of the RTBF by comparing the solutions implemented in other States, mostly in Latin America and Asia, in order to address the social need not to have life permanently exposed online and at the same time, taking into consideration the Freedom of Speech. This book is the result of an international cooperation launched through the first e-conference organized by blogdroiteuropeen in May-June 2017. It brings together papers from twenty legal academics. It is the first digital book of the Series Open Access Book edited by blogdroiteuropeen.

Olivia Tambou est Maître de Conférence HDR spécialisée en droit de l'Union européenne à l'Université Paris-Dauphine, PSL Research University, France. **Sam Bourton** is a PhD candidate and Associate Lecturer in Law at the University of the West of England, UK.

ISBN 978-99959-0-401-2

Collection Open Access Book
dirigée par Olivia Tambou

https://blogdroiteuropeen.com

COLLECTION OPEN ACCESS BOOK
DIRIGÉE PAR OLIVIA TAMBOU

E-COLLOQUES

LE DROIT À L'OUBLI EN EUROPE ET AU-DELÀ

THE RIGHT TO BE FORGOTTEN IN EUROPE AND BEYOND

Blog Droit Européen

Sous la direction d'Olivia Tambou et de Sam Bourton

Références électroniques:

Tambou O., Bourton S. (dir.), *Le droit à l'oubli en Europe et au-delà/ The Right to be Forgotten in Europe and Beyond*, Avril 2018, Luxembourg, Blogdroiteuropéen, Collection Open Access Book, 152 pages.

Disponible sur Internet : https://wp.me/p6OBGR-2QK

Bibliographic references:

Olivia Tambou, Sam Bourton (Eds.), *The Right to be Forgotten in Europe and Beyond/ Le droit à l'oubli en Europe et au-delà* (Series Open Access Book, Blogdroiteuropéen 2018)

Available at : https://wp.me/p6OBGR-2QK

ISBN 978-99959-0-401-2

Droit à l'oubli en Europe et au-delà
The Right To Be Forgotten in Europe and Beyond

Collection Open Access Book

Dirigée par Olivia Tambou

Sous la direction d'Olivia Tambou
et de Sam Bourton

Blog Droit Européen

SOMMAIRE
TABLE OF CONTENTS

SOMMAIRE
TABLE OF CONTENTS

SOMMAIRE
TABLE OF CONTENTS

SOMMAIRE
TABLE OF CONTENTS

SOMMAIRE
TABLE OF CONTENTS

LISTE DES ABRÉVIATIONS
LIST OF ABBREVIATIONS

Aff.	affaire
AEPD	Agence Espagnole de Protection des Données
AN	Audienca National
Art.	Article
Art.29 WP, A29WP	Article 29 Working Party
BDSG	Bundesdatenschutzgesetz
Cf.	confer
CE	Conseil d'Etat
CEDH	Convention Européenne des Droits de l'Homme
CELE	Freedom of Expression Centre of Study
CFR	Charter of Fundamental Rights of the EU
CJUE	Cour de Justice de l'Union Européenne
CJEU	Court of Justice of the European Union
civ.	civile
CNIL	Commission Nationale Informatique et Libertés
CPC	Code de Procédure Civile
CPDP	Computer Privacy Data Protection
DI	Datainspektion
DPA	Data Protection Authority
DSGVO	Datenschutz-Grundverordnung
GDPR	General Data Protection Regulation
EC	European Community
ECJ	European Court of Justice
ECLAC	United Nations Economic Commission for Latin America and the Caribbean
ECHR	European Convention of Human Rights

LISTE DES ABRÉVIATIONS
LIST OF ABBREVIATIONS

ECtHR	European Court of Human Rights
Eds	Editors
EEA	European Economic Area
EEE	Espace Economique Européen
e.g.	For example
EU	European Union
FAQ	Frequently Asked Questions
Fn.	Footnote
G29	Groupe de l'article 29
Ibid	In the same place/ in the same source
Ibidem	in the same place/ in the same source
ICO	Information Commissioner's Office
i.e. id est	In other words
INAI	National Institute of Transparency, Access to Information and Protection of Personal Data in Mexico
lit.	letter
OJ L	Official Journal Legislation
Ord.	Ordonnance
p., pp.	page, pages
para.	paragraph
RGPD	Règlement Général de la Protection des Données
RFDA	Revue Française de Droit Administratif
RTBF	Right To Be Forgotten
s.	suivante

LISTE DES ABRÉVIATIONS
LIST OF ABBREVIATIONS

et. seq.	et sequentia.
CSJN	Supreme Court of Justice of the Argentine Republic
TGI	Tribunal de Grande instance
TUE	Traité de l'Union européenne
TFEU	Treaty on the Functioning of the European Union
TFUE	Traité sur le Fonctionnement de l'Union Européenne
URL	Uniform Resource Locator
UE	Union Européenne
UK	United Kingdom

PRÉSENTATION DES ÉDITEURS
INTRODUCTION TO THE EDITORS

Olivia Tambou
Maître de Conférences HDR spécialisée en droit de l'Union européenne à l'Université Paris-Dauphine, PSL Research University, Cr2D

Olivia Tambou is Associate Professor at the Paris-Dauphine University specialized in European Law. She has been lecturing in French and foreigner Universities for more than 20 years. Her current research interest is the effectiveness of the European Data protection Law. She wrote several articles on the General Data Protection Regulation (GDPR) about certification, remedies, profiling and the de-listing right. She is a contributor of the comparative section of the European Data Protection Law (EDPL) regarding data protection issues in France . She is also the editor of blogdroiteuropeen. Olivia Tambou has a LLM from Kiel Albrecht University (Germany), a PhD in European Law from the Law faculty of Strasbourg. She received a Marie Curie Scholarship from the European Commission for her post-doctoral research at the Universitat Autònoma of Barcelona. Her main scientific interest lies in legal pluralism (relationships between state legal orders in the EU, transfrontier cooperation, harmonisation, regulation).

Olivia Tambou est Maître de Conférences HDR en droit à l'Université Paris-Dauphine, PSL Research University. Elle enseigne depuis plus de vingt ans dans des universités en France et à l'étranger. Sa thématique actuelle de recherche porte sur l'effectivité du droit européen de la protection des données personnelles. Elle a écrit plusieurs articles sur le Règlement Général de la Protection des Données (RGPD) notamment sur la certification, les recours, les sanctions, le profilage et le droit au déréferencement/droit à l'oubli. Elle est contributrice de la section comparative de la European Data Protection Law (EDPL) en ce qui concerne la protection des données en France. Elle est aussi l'éditrice de blogdroiteuropeen. Olivia Tambou dispose d'un LLM de l'Université de Kiel (RFA), d'un doctorat en droit communautaire de la faculté de droit de Strasbourg sur *Les rapports entre l'ordre juridique communautaire et les ordres juridiques français et allemand*. Elle a reçu une bourse post-doctorale pour son travail sur la coopération transfrontière à l'échelle de la Catalogne réalisée à l'Université Autonome de Barcelone. Elle s'intéresse globalement au pluralisme juridique européen (rapports entre les ordres juridiques, coopération transfrontière, harmonisation, régulation).

Sam Bourton
Associate Lecturer in Law, University of the West of England

Sam Bourton is a PhD candidate and an Associate Lecturer in Law at the University of the West of England. She lectures on several undergraduate and postgraduate modules including, Foundations for Law, Law of Financial Crime and Regulation, and International Financial Crime. Her research focuses on the law of financial crime, particularly tax evasion and money laundering, and she has written several articles on these topics.

PRÉSENTATION DES CONTRIBUTEURS
INTRODUCTION TO THE CONTRIBUTORS

Pedro Anguita Ramírez

Pedro Anguita Ramirez is a Professor at the School of Communication, Universidad de los Andes, Chile.

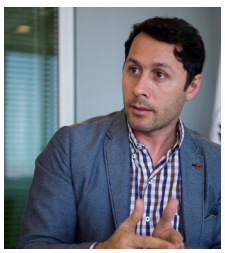
To contact, e-mail panguita@uandes.cl

Paul Bernal

Paul Bernal is a Senior Lecturer in Information Technology, Intellectual Property and Media Law at the UEA Law School, University of East Anglia.

Cyril Cohendy

Cyril Cohendy is a holder of an LL. M. and a Master 2 in European law; Currently a PhD student at the Université Paris 1 Panthéon-Sorbonne on a mission to the French University College of St. Petersburg. His thesis deals with the financing of energy interconnection in Europe.



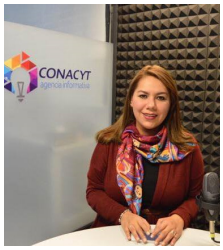
Juan Gustavo Corvalán

Juan Gustavo Corvalán is a lawyer by the University of Buenos Aires (UBA). He is also a Doctor in Legal Science, and currently, he is a postdoctoral and visiting professor in the Master in Digital Law at Université Panthéon-Sorbonne - Paris 1. He is a Specialist in Tax Law by the Austral University, and a professor of Administrative Law at the undergraduate and postgraduate level at the University of Buenos Aires. He is a judge of the Administrative and Tax Litigation Law of the City of Buenos Aires, position obtained through contest and qualifications assessment, and is currently working as Deputy General Prosecutor in Administrative and Tax Litigation before the Superior Court of Justice of the City of Buenos Aires. He is the author of four books and has published more than sixty articles in Argentina and abroad. He has also given more than a hundred lectures in different cities around the world. He is the Director of an electronic legal newspaper, called DPI Journal, and has led the development of "Prometea", the first artificial intelligence at the service of rights that is currently being applied.

PRÉSENTATION DES CONTRIBUTEURS
INTRODUCTION TO THE CONTRIBUTORS

Pierre-Luc Deziel

Pierre–Luc Déziel est professeur adjoint à la Faculté de droit de l'Université Laval, au Québec. Ses intérêts de recherche se situent au carrefour du droit à la vie privée et des technologies de l'information.



Olivia Andrea Mendoza Enríquez

Olivia Andrea Mendoza Enríquez is a full-time Research Professor at the Public Research and Innovation Center, in Information and Communication Technologies INFOTEC.
To contact, email olivia.mendoza@infotec.mx

David Erdos

David Erdos is University Senior Lecturer in Law and the Open Society and Deputy Director of the Centre for Intellectual Property and Information Law (CIPIL) at the Faculty of Law, University of Cambridge.

David's research focuses on the nature of data protection especially as this interacts with freedom of expression. Drawing on a background in both law and political science, his work has developed arguments about the nature, substance and operation of the law using not only traditional doctrinal analysis but also both quantitative and qualitative empirical methodology.

Silvio Luis Ferreira da Rocha

Silvio Luis Ferreira da Rocha est professeur de droit administratif et de droit civil à l'Université Catholique de São Paulo – PUC / SP. Ancien conseiller du Conseil National de Justice, il est juge fédéral à São Paulo. Auteur de plusieurs ouvrages et articles publiés au Brésil et à l'étranger.

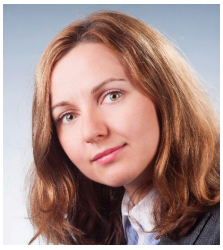
Shizuo Fujiwara

Shizuo Fujiwara is a Professor at Chuo Law School, Chuo University. Shizuo specializes in Administrative Law, Information Law and Local Autonomy Law.

PRÉSENTATION DES CONTRIBUTEURS
INTRODUCTION TO THE CONTRIBUTORS

Piao-Hao Hsu

Piao Hao Hsu is currently a Lecturer at International School of Technology and Management, Feng Chia University, Taichung. From 2013 to 2017, he worked as Legal Researcher at Science and Technology Law Institute (STLI), Institute for Information Industry, where he is responsible for policy research in the field of energy law and innovative technology. It is also during his post at STLI, that he started his research on RTBF. Prior to STLI, Hsu also worked as Senior Assistant Research Fellow at Taiwan Research Institute (TRI) and Program Associate at Human Rights in China (Hong Kong Office). In addition to being a Ph.D. candidate of Graduate Institute of European Studies, Tamkang University, Taipei, Hsu holds LL.M. (Master of Law) from the University of Amsterdam, the Netherlands and LL.B. from National Taiwan University, Taiwan.



Agnieszka Janczuk-Gorywoda

Agnieszka Janczuk-Gorywoda is an Assistant Professor in European Economics Law, Utrecht University, Law School.

Patricia Jonason

Patricia Jonason is an Associate Professor in the Public Law Department at Södertörn University, Stockholm, Sweden. Law. She teaches administrative and constitutional law as well as European law and Human Rights. Her current main research interests are on privacy and on the right of access to information.

Konstantinos Margaritis

Konstantinos Margaritis is an Adjunct Lecturer in the Department of Political Science at the University of Crete. Konstantinos is an Attorney at Law and member of the Governing Board of the Hellenic Association of Public Law.

Miquel Peguera

Miquel Peguera is an Associate Professor of Law at Universitat Oberta de Catalunya (UOC) (Barcelona, Spain). Miquel is an Affiliate Scholar at the Stanford Center for Internet & Society. His research focuses on intermediary liability, copyright, trademarks, and privacy.

PRÉSENTATION DES CONTRIBUTEURS
INTRODUCTION TO THE CONTRIBUTORS

Enrico Peuker

Enrico Peuker is a Post-Doc at Humboldt-University of Berlin. His research focusses on German and European Administrative Law, German and European Constitutional Law, Constitutional Aspects of Digitalization, German and European Data Protection Law. Contact: enrico.peuker@rewi.hu-berlin.de
https://www.rewi.hu-berlin.de/de/lf/ls/rft/team/ep

Olivia Tambou

Olivia Tambou est Maître de Conférence HDR spécialisée en droit de l'Union européenne à l'Université Paris-Dauphine, PSL Research University.

Giulia Tiberi

Giulia Tiberi is Adjunct Professor of Constitutional Law at the University of Insubria (Italy, Varese-Como (giulia.tiberi@uninsubria.it). Academic Coordinator and Module Leader of the following Jean Monnet Modules: "Personal data protection as a fundamental right in the EU in the digital age - A dialogue among constitutional law, criminal law, civil procedure law and judicial protection of IP rights" (2015-2018); "The protection of fundamental rights in the evolution of the European integration process" (2008-2011).

Rafael Valim

Rafael Valim est Professeur de droit administratif et de fondements du droit public à l'Université Catholique de São Paulo – PUC / SP. Auteur de plusieurs ouvrages et articles publiés au Brésil et à l'étranger. Son dernier ouvrage est intitulé « État d'exception: la forme juridique du néo-libéralisme » (São Paulo: Contracorrente, 2017).

Pieter Van Cleynenbreugel

Pieter Van Cleynenbreugel is a Professor of European Union law at the Faculté de Droit, de Science Politique et de Criminologie of the University of Liège, where he is also the Directeur of the Institut d'Etudes Juridiques Européennes and a Fellow of the Liège Competition and Innovation Institute. His research and publications focus on EU internal market law.

Nicolo Zingales

Nicolo Zingales is a Lecturer in Competition and Information Law at the School of Law, Politics and Sociology, University of Sussex.

REMERCIEMENTS
ACKNOWLEDGEMENTS

REMERCIEMENTS

Cet ouvrage est le fruit d'une e-conférence qui s'est déroulée en mai-juin 2017 sur blogdroiteuropéen et qui a consisté à la publication quotidienne de posts ou de Working papers. Il réunit la plupart des contributions mises à jour avec quelques nouvelles contributions visant à mieux couvrir son champ d'étude. Nos premiers remerciements vont à l'ensemble de ces vingt auteurs pour leur intérêt à participer à cet ouvrage numérique. Olivia Tambou tient à remercier les membres de l'équipe de blogdroiteuropéen qui sont intervenus activement dans le bon déroulement de cette e-conférence à travers leurs relectures et traductions en particulier, Lise Fogel, Elise Daniel, Catherine Warin, ainsi que Nicolas Bremand pour ses commentaires constructifs. Olivia Tambou tient également à remercier Vlad Titerlea et Thomas Perennou pour leurs relectures finales. Blogdroiteuropéen souhaite remercier Juan Gustavo Corvalàn dont l'aide a été précieuse pour la recherche d'auteurs latino-américains, ainsi que P.Y. Monjal pour sa mise en relation avec le Professeur Shizuo Fujiwara. Blogdroiteuropéen souhaiterait également exprimer sa gratitude envers Maryline Boizard et Cristina Pauner pour le soutien scientifique qu'elles ont apporté à cette e-conférence. Blogdroiteuropéen tient aussi à saluer Mme Aurelie Bretonneau, rapporteure publique au Conseil d'Etat, qui a généreusement accepté la publication en libre accès de ses conclusions dans l'affaire *Google c. Cnil*, (see Annex 1). Enfin, une dédicace spéciale à Cathy Ley qui a réalisé la couverture de cet ouvrage et dont les conseils de mise en page ont été précieux.

ACKNOWLEDGEMENTS

This book is the result of an e-conference, which took place in May-June 2017 on blogdroiteuropéen with a daily publication of posts or Working Papers. It includes most of these contributions, which have been updated, and some additional papers in order to improve the scope of the analysis. Our first acknowledgements are dedicated to our twenty authors for their interest in participating in this digital book. Olivia Tambou would like to thank members of the blogdroiteuropéen's team who were involved in the organization of this e-conference in particular Lise Fogel, Elise Daniel, Catherine Warin for their proofreading and translation, and Nicolas Bremand for his constructive feedback. Olivia Tambou would also like to thank Vlad Titerlea and Thomas Perennou for their final proofreading. Blogdroiteuropeen is particularly grateful for the assistance given by Juan Gustavo Corvalàn in the search of Latin American authors, as well as P.Y. Monjal for the contact with Professeur Shizuo Fujiwara. Blogdroiteuropéen wish to acknowledge Maryline Boizard and Cristina Pauner for their scientific support to this e-conference. Blogdroiteuropéen would like to express gratitude to Aurelie Bretonneau, public rapporteur at the French Conseil d'État who generously accepted to edition in Open Access her conclusions in the *Google V. Cnil Case*. (see Annex 1.) Last but not least, blogdroiteuropéen would like to offer special thanks to Cathy Ley, who realized the cover of this new Series Open Access Book and gave us precious advice for the edition.

PROPOS INTRODUCTIFS

par Olivia Tambou
Maître de Conférences HDR spécialisée en droit de l'Union européenne à l'Université Paris-Dauphine, PSL Research University, Cr2D

Cet ouvrage interroge l'impact de l'arrêt *Google Spain c. Costeja*, quatre ans après son adoption. Il s'agit de comprendre comment ce droit à la nature ambiguë est mis en oeuvre par Google, mais aussi par les autorités de protection et les juridictions au sein d'Etats membres de l'UE. Cet ouvrage questionne également les futures évolutions du droit à l'oubli numérique en Europe. Il invite à mieux saisir l'ancrage européen de ce droit en confrontant les solutions mises en place dans d'autres Etats principalement en Asie et en Amérique Latine pour répondre au besoin social de ne pas voir son histoire personnelle affichée de manière permanente sur Internet tout en protégeant la liberté d'expression.

Googliser est aujourd'hui une pratique courante au point que ce terme est entré dans le Dictionnaire Larousse qui le définit comme l'activité de «rechercherdesinformations(enparticuliersurquelqu'un) sur Internet en utilisant le moteur de recherche Google ». Les moteurs de recherche nous facilitent un accès mondial à l'information. Ils jouent un rôle essentiel dans le développement d'une société de la connaissance fondée sur la diffusion des savoirs. Toutefois, cela ne doit pas se faire au détriment du respect de la vie privée et de la protection de nos données personnelles. Adopté, il y a quatre ans, l'arrêt *Google Spain c. Costeja* propose de concilier et de hiérarchiser ces droits fondamentaux. Il est l'illustration d'une réponse européenne à un besoin social universel inhérent au développement de l'internet: celui de pas voir certaines informations personnelles perpétuellement exposées sur Internet par un accès facilité par les moteurs de recherche. Il faut rappeler que dans l'arrêt Google Spain c. Costeja[1], la voie choisie ainsi que l'étendue de la réponse de la CJUE ont été encadrées par l'objet de la saisine. Il s'agissait de savoir si un moteur de recherche pouvait refuser la demande d'une personne visant à la suppression des liens permettant d'accéder, en faisant une recherche à partir de son nom, à une page comportant une information licite mais ancienne dont le traitement ne lui apparaissait plus pertinent[2].

La CJUE a répondu par la négative tout en soumettant la mise en œuvre de son arrêt à une régulation par les moteurs de recherche sous le contrôle des autorités de protection des données personnelles et en dernier recours des juges. Entre temps le législateur européen, après quelques hésitations a fait le choix de consacrer à l'article 17 du Règlement Général de la Protection des Données (RGPD),[3] le droit à l'effacement et à l'oubli numérique. Cela pose la question de l'articulation de ce droit à l'oubli numérique, avec la jurisprudence Google qui consacre un droit au déréférencement.

Quatre ans après l'arrêt *Google Spain c. Costeja*, la nature même du droit consacré ainsi que son régime sont encore en construction en Europe, tout en faisant aussi débat à l'échelle mondiale. L'objet de ces propos introductifs n'est pas d'apporter des réponses à

[1] CJUE 13 mai 2014, aff. 131/12, Google Spain SL, Google Inc. c/ Mario Costeja González e.a., non encore publié au Recueil, ECLI:EU:C:2014:317; Artemi Rallo, The Right to Be Forgotten on the Internet: Google v. Spain, Electronic Privacy Information Center 2018
[2] L'origine espagnole d'un besoin au droit au déréférencement est née à la suite de la numérisation des archives des journaux officiels et de la presse classique. Cette numérisation a permis aux internautes de faire resurgir le passé de personnes en googlisant leurs noms. Les premiers cas de requête adressées à l'AEPD , Agence Espagnole de Protection des Données datent ainsi de 2007. Les requérants souhaitaient principalement supprimer cet accès par Google et non pas véritablement la suppression de l'information dans le site originel. Pour une analyse approfondie des différents premiers cas dont a été saisis l'AEPD cf. A. Rallo, *El derecho al olvido en Internet, Google versus España*, Centro de Estudios Politicos y Constitutionales, Madrid 2014, cf. aussi la vidéo de sa conférence sur le droit à l'oubli en ligne : l'expérience espagnole donnée le 30 novembre 2015 à l'Université Paris-Dauphine, spécialement à partir de la minute 4'57.
[3] Règl. n° 2016/679, 27 avr. 2016 : JOUE n° L 199, p. 1.

l'ensemble de ces questionnements qui seront abordés dans les contributions futures mais d'expliquer la raison d'être de cet ouvrage en rappellant quelques premisses conceptuelles (I) justifiant la nécessité d'une analyse contextuelle du droit à l'oubli en Europe et au-delà. (II)

I-LES PREMISSES CONCEPTUELLES DE CET OUVRAGE

Trois constats peuvent être dressés. Premièrement, l'arrêt *Google Spain* constitue l'affirmation nuancée d'un droit au déréférencement par la CJUE, même si la nature de celui-ci est équivoque. La pluralité de vocabulaire en témoigne. Si l'expression « droit à l'oubli » est utilisée[4], la doctrine utilise surtout le terme « de droit au déréférencement »[5], (*delisting right* en anglais) plus rarement celui de desindexation (*derecho a la desindexación* en espagnol), et plus récemment celui de « droit à l'obscurité »[6], (*right to obscurity*). Deuxièmement, ce droit fait l'objet d'une utilisation effective par ses destinataires. Troisièmement, la mise en œuvre de ce droit par les régulateurs demeure peu transparente.

A- L'affirmation nuancée d'un droit au déréfencement

1°) D'un droit au déréférencement à un droit à l'obscurité

L'arrêt Google consacre un nouveau droit qui permet à un individu de se tourner directement vers un moteur de recherche afin d'obtenir la suppression de l'accès à l'information révélant ses données personnelles dès lors que le traitement de celles-ci ne repose plus sur un fondement légitime. L'information demeure en ligne, mais elle sera plus difficilement trouvable du fait de la disparition des liens dans le moteur de recherche. Autrement dit, ce droit s'impose aux moteurs de recherche mais pas nécessairement aux éditeurs de site web qui sont à l'origine de ces contenus. La Cour invoque une triple justification à cette différence de traitement. D'une part, elle est liée à l'importance actuelle de l'utilisation d'un moteur de recherche pour accéder à une information[7]. La Cour en déduit que cette mise en relation est le plus souvent à l'origine d'une ingérence plus grande dans les droits protégés que celle découlant du traitement originel par le site web en cause. Elle y voit une « affectation additionnelle des droits fondamentaux de la personne concernée »[8], qui justifie l'obligation spécifique imposée aux moteurs de recherche. D'autre part, elle permet de couvrir l'hypothèse où l'éditeur n'est pas connu ou est difficilement accessible parce qu'en dehors de l'Union européenne[9]. Enfin, cela permet également de s'appliquer à des hypothèses où l'information originelle ne peut pas véritablement faire l'objet d'une désindexation parce qu'il s'agit d'une obligation légale.[10] S'adresser au moteur de recherche constitue une solution permettant d'assurer une protection que la Cour considère alors comme « efficace et complète » parce qu'elle n'exige pas de saisir d'abord l'éditeur de contenu.

L'arrêt *Google Spain* crée ainsi un droit-procédure: le droit de demander aux moteurs de recherche de supprimer la mise en relation vers des URLs sur internet obtenus par une recherche comportant des données personnelles d'un individu. Il comporte également une nouvelle obligation pour les moteurs de recherche en tant que responsable de traitement de données personnelles. En effet, dans son arrêt *Costeja* la CJUE a considéré que l'activité de collecte, d'enregistrement et d'organisation pour indexation et ensuite de mise à disposition des utilisateurs de listes de résultats de données permettant d'identifier une personne constitue un traitement de données personnelles. En outre, l'exploitant d'un moteur de recherche déterminant lui-même les finalités de ces traitements et les moyens de son activité, il n'est pas un simple intermédiaire technique.

La lecture de l'arrêt ne permet pas de comprendre quelle est la nature véritable du droit consacré. La CJUE s'est d'ailleurs bien gardée de le définir par un terme spécifique. Il s'agirait d'un droit hybride. La CJUE le rattache conjointement au droit d'accès (art.12 b) qui

[4] Pour une analyse pluridisciplinaire du droit à l'oubli en France, cf. M. Boizard , Le droit à l'oubli, recherche réalisée avec le soutien de la Mission de recherche Droit et Justice, févr. 2015, accessible https://halshs.archives-ouvertes.fr/halshs-01223778/document

[5] O.Tambou, Protection des données personnelles: les difficultés de la mise en œuvre du droit européen au déréférencement. *Revue trimestrielle de droit européen*, 2016, 2016 (2). <hal-01408535

[6] Expression due à Julie Brill, Federal Trade Commissioner, voir par exemple Why do you have the right to obscurity, by E. Selinger and W/ Hartzog, Aprit 15, 2015 accessible à https://www.ftc.gov/system/files/documents/public_statements/637101/150415righttoobscurity.pdf

[7] Point 80

[8] Point 83

[9] Point 84

[10] Point 85

[11] Il faut souligner sur ce point que la CJUE est allée au-delà de la position de l'AEPD qui à l'origine fondait le droit au déréférencement sur le droit à l'opposition cf. sur ce point Rallo A., ouvrage précité spécialement p. 174

évoque l'effacement et le verrouillage des données et au droit d'opposition (article 14a) de la directive 95/46[11]. L'usage du terme de droit au déréférencement a alors été proposé afin de rendre compte de ce nouveau droit étant donné qu'il était cantonné aux moteurs de recherche et qu'il comportait des spécificités par rapport aux droits d'effacement et d'opposition. D'une part, le droit d'effacement et le droit d'opposition ne réclament pas de conditions temporelles pour leur application. D'autre part, l'exercice du droit d'opposition nécessite la preuve de « raisons prépondérantes et légitimes tenant à la situation particulière de la personne intéressée » (Art. 14 a) de la directive 95/46). Enfin, le droit d'effacement exige de son côté que le traitement ne soit pas conforme à la directive. Dans ce cas la suppression est de droit.

Trois ans après, le récent arrêt *Manni*[12] atteste qu'au-delà des moteurs de recherche les individus peuvent obtenir d'autres acteurs la limitation de l'accès par des tiers à des données personnelles qu'ils traitent, à l'issue d'un certain délai dans des conditions très particulières sur lesquelles nous reviendrons ultérieurement. En l'espèce, il s'agissait des autorités en charge des registres des sociétés. A ce stade ce qu'il est important de retenir, c'est l'analogie entre le droit consacré par l'affaire Google et celui en cause dans l'affaire *Manni*[13]. Dans cette seconde affaire le terme de déréférencement semble difficilement utilisable, celui-ci étant étroitement lié à l'activité des moteurs de recherche. En revanche, celui de droit à l'obscurité serait sans doute plus pertinent pour transcrire l'idée que des individus peuvent obtenir de certains responsables de traitement de données personnelles une limitation de l'accès à leurs données personnelles par des tiers. Le terme de droit à l'obscurité a le mérite de laisser ouverte l'épineuse question quant à savoir comment techniquement cette obscurité est ou doit être réalisée par le responsable de traitement: effacement-suppression des données personnelles ou blocage d'accès à ces données qui restent stockées sur son serveur. Le terme de droit à l'obscurité traduit bien également que les données personnelles demeurent présentes dans un recoin d'Internet mais qu'elles ne peuvent pas être vues de tous. L'article 17 du RGPD consacre lui explicitement un droit à l'oubli numérique rattaché à un droit à l'effacement. Cette disposition prévoit une obligation d'effacement à la charge du responsable en cas d'absence de fondement légitime du traitement qui peut prendre plusieurs formes : l'absence de nécessité, le retrait du consentement, l'exercice d'un droit d'opposition, illicéité du traitement[14], l'existence d'une obligation légale. Cependant à aucun moment ce droit à l'oubli n'est explicitement défini. Il n'est même pas fait mention de sa caractéristique existentielle et distinctive pour le déclencher c'est-à-dire la prise en compte d'un délai certain rendant ainsi le traitement des données illégitimes. Il est possible d'augurer que la jurisprudence *Google Spain* continuera à être prise en compte dans l'interprétation de l'article 17 du RGPD à l'avenir.

Cette disposition a été citée par l'Avocat Général Bot dans ses conclusions[15] afin de rappeler que, la cohérence entre la solution dégagée dans l'arrêt *Manni* avec cette disposition qui prévoit l'absence de droit à l'effacement lorsque le traitement est, nécessaire pour respecter « une obligation légale … ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement » et ou à « des fins archivistiques dans l'intérêt public ». L'affirmation d'un droit oubli numérique par la CJUE comme par le RGPD n'est donc pas absolue.

2°) De la nuance avant toute chose

Le droit au déréférencement a été d'emblée conçu comme un droit qui n'est pas absolu, dès lors qu'il est fondé sur le droit à la protection des données personnelles qui lui-même n'est pas absolu. Si cette nuance n'a pas toujours été perçue ou comprise dans l'arrêt *Google Spain*, elle est très présente en revanche dans l'affaire *Manni*. Dans le premier cas, la CJUE a consacré un droit au déréférencement qui semble être le principe tout en envisageant de possibles limitations. Dans le second cas, la CJUE a relevé

[12] CJUE 9 mars 2017, Camera di Commercio c. S. Manni, aff. C-398/15, non encore publié au Recueil, ECLI:EU:C:2017:197
[13] Cette analogie est d'autant plus éclatante si l'on prend en compte les conclusions de l'Avocat Général Bot. Ce dernier s'est déclaré opposé à la reconnaissance de toute possibilité de droit à l'obscurité. A l'appui de sa démonstration il considère que « Le choix que font des personnes physiques de s'engager dans la vue économique par l'intermédiaire d'une société commerciale implique une exigence permanente de transparence »… le traitement de leurs données personnelles dans les registres de sociétés est justifié « par un intérêt prépondérant des tiers à avoir accès aux informations en question » (point 100). Il s'agit là de l'application d'une exception dégagée par la CJUE dans son arrêt Google Spain.
[14] Cela concerne en particulier l'hypothèse de traitement de données personnelles de mineurs dans le cadre des services de la société de l'information sans l'autorisation parentale requise à l'article 8 §1, forme d'illicéité explicitement et séparément visée.
[15] Point 101

l'absence de principe à un droit à l'obscurité des données personnelles figurant dans le registre des sociétés tout en laissant la possibilité d'exceptions acceptées par les Etats membres au cas par cas. Cette différence d'approche est essentiellement liée à la finalité même du traitement envisagé. Le traitement fait par Google de nos données personnelles n'est pas en soi considéré comme un traitement présentant un intérêt public. La preuve en est qu'il n'existe pas en soi de droit au référencement. En revanche, l'inscription des données personnelles dans les registres de sociétés répond bien à un intérêt public de transparence, de sécurité juridique : protéger les intérêts des tiers. Les sociétés par action et les sociétés à responsabilité limitée n'offrent comme garantie à l'égard des tiers que leur patrimoine social. Dans ces conditions connaître l'identité des personnes dirigeantes constitue une information présentant un intérêt légitime.

Dans l'arrêt *Google Spain*, la CJUE s'est clairement prononcée pour la prévalence de principe de la protection des données personnelles[16]. Elle a établi une hiérarchie des intérêts à prendre en compte dans la mise en œuvre du droit au déréférencement. D'une part, elle affirme le principe de la prévalence des droits de la personne concernée sur l'intérêt économique du moteur de recherche. Le seul intérêt économique du moteur de recherche ne peut à lui seul servir de fondement légitime au maintien d'un traitement[17]. D'autre part, elle affirme également la prévalence de principe des droits des personnes protégées sur l'intérêt des internautes au maintien de l'information comportant des données personnelles[18]. Enfin, elle considère que cette présomption peut être renversée. Des raisons particulières peuvent justifier « un intérêt prépondérant du public » à avoir accès de cette information. Ces raisons peuvent être liées à la nature particulière de l'information, au rôle joué par la personne dans la vie publique, au temps écoulé rendant l'information plus pertinente etc.

Dans l'arrêt *Manni*, la CJUE considérant d'emblée l'intérêt public du traitement des données personnelles dans les registres des sociétés s'appuie également sur le droit à l'opposition et le droit d'effacement. La CJUE concède sur ce fondement une possibilité très réduite pour les autorités nationales en charge de ces registres des sociétés de limiter à titre exceptionnel l'accès à ces données personnelles à l'issue d'un délai suffisamment long suite à une requête en ce sens d'un individu. Une telle possibilité ne peut être exercée que dans des circonstances particulières comportant des raisons prépondérantes et légitimes. En outre, les Etats membres peuvent supprimer cette possibilité. La CJUE l'a rappelé en soulignant que le droit à l'opposition peut être mis en cause par une obligation légale de traitement.

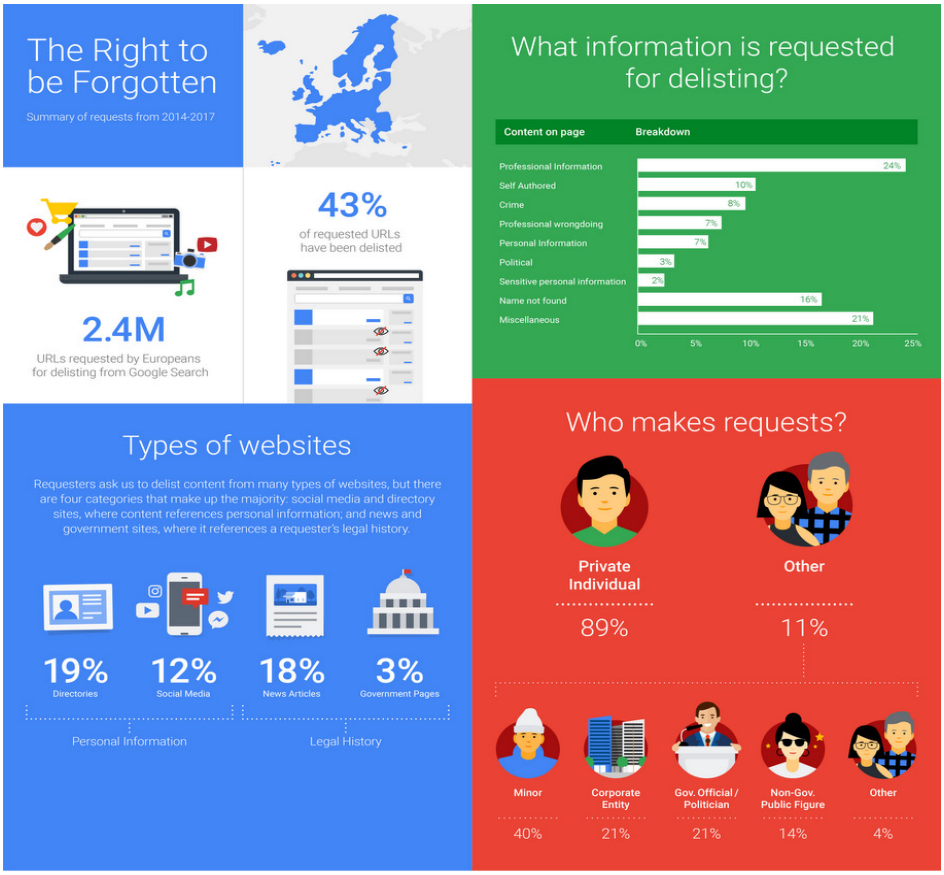
Dans ces deux arrêts on retrouve ainsi la nature hybride du droit à l'obscurité entre droit d'opposition et droit d'effacement dont l'exercice est subordonné à l'écoulement d'un délai certain. Dans les deux cas, il s'agit d'un droit pondéré nécessitant de faire une balance des intérêts et dont l'exercice est soumis à un contrôle de proportionnalité.

B- L'utilisation effective du droit au déréférencement par ses destinataires

Selon les professeurs Ost et De Kerchove, « *est effective la règle utilisée par ses destinataires comme modèle pour orienter leur pratique* »[19]. Le droit au déréférencement comporte quatre types de destinataires : les individus, les moteurs de recherches, les autorités administratives indépendantes et les juges. Chacun de ces acteurs a pris en compte l'existence de ce nouveau droit.

Les moteurs de recherche ont accepté la fonction que leur a assigné la CJUE de régulation du droit au déréférencement. Google a très rapidement mis à disposition des individus un formulaire en ligne leur permettant d'exercer leur droit[20]. Il a aussi mené une véritable opération de responsabilité sociétale afin d'entendre des experts pour orienter la manière dont il devait mettre en œuvre ce droit[21]. Par ailleurs, les

[16] Point 81
[17] Point 81 et point 97
[18] Point 81
[19] Ost F., et van De Kerchove M., De la pyramide au réseau, pour une théorie dialectique du droit, 2002, publication universitaire des facultés de Saint Louis, sp. p. 330.
[20] Le formulaire de Google est accessible ici , celui de Bing, là.
[21] Voir notre tribune, Le rapport du Comité Google: exercice d'autorégulation d'un droit à l'oubli, Dalloz Actualité, Droits en Débats, 19 fev. 2015,
[22] Cf. la note adressée à la Federal Trade Commission par l'association Consumer Watchdog le 7 juillet 2015, acecssible à http://www.consumerwatchdog.org/resources/ltrftcrtbf070715.pdf; La presse fait écho du dépôt de proposition visant à assurer un droit à l'oubli dans l'Etat de New York, cf. E. Volokh, N.Y. bill would require people to remove 'inaccurate', 'irrelevant', 'inadequate' or 'excessive' statements about others



moteurs semblent avoir mis en place des solutions techniques pour permettre l'exercice de ce droit à l'obscurité, alors même qu'à l'origine leur opposition était notamment liée à l'impossibilité technique de le mettre en œuvre. La capacité révélée au grand public de Google à mettre en œuvre techniquement ce droit au déréférencement a notamment été à l'origine de la revendication d'acteurs américains pour l'introduction d'un tel droit dans leur propre pays[22].

Les statistiques actuellement disponibles[23] attestent également que les individus exercent leur droit au déréférencement. Les requêtes sont originaires de l'ensemble des pays de l'Espace économique européen. La France, l'Allemagne, la Grande-Bretagne, l'Espagne et l'Italie arrivent néanmoins en tête des pays dans lesquels les demandes ont été les plus importantes. Deuxièmement, le nombre important de déréférencements opérés par Google atteste que ce droit répond aussi à un besoin juridique. 43% des demandes ont donné lieu à un déréférencement. Cela signifie que ce droit permet de rendre plus effective la protection des données personnelles. Troisièmement, le nombre de cas dans lesquels Google et les autorités nationales de protection des données personnelles auraient été en désaccord semble relativement limité[24]. La seule véritable opposition de principe tient au champ d'application géographique du droit au déréférencement. La CNIL est partisane d'une application mondiale[25] alors que Google lui oppose que ce droit est applicable uniquement en Europe et à partir de l'utilisation du moteur de recherche en Europe[26]

Malgré cela, la réalité des usages des acteurs (moteurs

[23] Cf. la page dédiée pour Google : http://www.google.com/transparencyreport/removals/europeprivacy/ et celui de Microsoft https://www.microsoft.com/en-us/about/corporate-responsibility/crrr
[24] Le chiffre de 1% des cas ayant fait l'objet d'un appel devant une autorité de protection des données ont été annoncés par Peter Fleischer lors de la CPDP 2017.
[25] Pour une présentation de cette vision par la Présidente de la CNIL cf. Pour un déréférencement mondial, Tribune d'Isabelle Falque-Pierrotin publiée dans les pages Débats du Monde du 29 décembre 2016 ou encore The Right to obscurity : implementing the Google-Spain Decision, round table at the Computer, Privacy, and Data Protection (CPDP) 2017, à partir de la minute 29'24
[26] Pour une présentation de cette vision par Peter Fleischer cf. vidéo précitée, à partir de la minute 19'51

de recherche, individus) atteste que le droit au déréférencement bénéficie d'une effectivité certaine. Ce premier constat demande bien sûr à être nourri et étayé de façon plus précise. Le rôle des autorités administratives indépendantes et des juges dans la mise en œuvre du droit à l'oubli se doivent d'être mieux cernés. C'est précisemment l'objectif de cet ouvrage. Il faut néanmoins d'emblée souligner que cette entreprise est difficile car la mise en œuvre du droit au déréférencement par les régulateurs est peu transparente.

C- La mise en œuvre peu transparente du droit au déréférencement par les régulateurs

Quatre ans après l'arrêt *Google Spain*, il demeure impossible de mener une étude empirique sur la mise en œuvre du droit au déréférencement. L'absence de transparence dans la manière dont les moteurs de recherche notamment Google traitent ces demandes a été maintes fois décriées[27], mais les choses n'ont guerre évolué[28].

L'absence de transparence des autorités de protection des données dans le traitement des requêtes, quoique moins soulignée, interroge tout autant. Une coordination entre les autorités de protection des données dans le traitement de leur demande de déréférencement a pourtant été mise en place[29]. Ces informations demeurent à usage interne. Aucune statistique globale, détaillée et à jour n'est livrée par le Groupe 29[30]. La production de communiqués de presse ainsi que de lignes directrices a été privilégiée. Mais là aussi, les lignes directrices pour l'application de l'arrêt *Google Spain* datent de 2014[31] et n'ont pas été mises à jour depuis 2015[32], notamment au regard de certaines difficultés rencontrées ou du nouvel article 17 RGPD. La priorité de ces autorités administratives indépendantes n'est pas la transparence de leur traitement du droit au déréférencement. Si on peut le comprendre, on peut néanmoins le regretter. Ces trois constats ont été à l'origine de la nécessité de présenter un ouvrage réalisant une analyse contextuelle du droit à l'oubli numérique en Europe et au-delà.

II- LA NÉCESSITÉ D'UNE ANALYSE CONTEXTUELLE DU DROIT À L'OUBLI

Une telle analyse se devait de commencer par une série d'articles permettant d'appréhender la mise en oeuvre nationale de l'arrêt *Google Spain*. (Partie 1). Il s'agissait ensuite de s'interroger de manière plus prospective sur la valeur ajoutée de la reconnaissance d'un droit à l'oubli numérique (Partie 2). Enfin, il fallait rendre compte de l'ancrage européen du droit au déréférencement qui ne trouve pas son pendant dans les autres pays du monde étudiés. La partie 3 de cet ouvrage témoigne de l'absence de réelles alternatives trouvées dans ces pays à la reconnaissance d'un droit à l'oubli numérique. Le déréférencement dans ces Etats est le plus souvent subordonné à la constatation, de l'illégalité du contenu vers lequel les liens renvoient, et/ou la démonstration de l'existence d'un dommage.

A- La diversité des approches nationales du droit au déréférencement

Cette première partie permet de renseigner de manière fine l'existence au delà d'une approche commune de points de divergences entre les Etats ou même à l'intérieur des Etats en ce qui concerne la mise en oeuvre de l'arrêt *Google Spain*. Plusieurs contributions (Miquel Perguera, Olivia Tambou, David Erdos, Giulia Tiberi) attestent de l'absence d'unanimité autour de la position de la CNIL en ce qui concerne la revendication d'un droit mondial au dérérenfencement. L'autorité espagnole accepte la solution proposée finalement par Google visant à geobloquer les URLs concernées qui ne peuvent plus être assessibles par les Européens, mais le demeurent dans les autres parties du monde. La Chambre civile de la Cour Suprême espagnole considère que la demande de déréferencement peut être adressée

[27] Sur ce point cf. notre article précité sur les difficultés de la mise en œuvre du déréférencement sp. p. 270 et s.
[28] Voir les élements fournis par Google en février 2018 se sont un peu étouffés.
[29] Cf. *Best Practices for cooperation between EU DPAs*, deliverable 2.2. January 2016, spéc. p. 10 et s. Http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA-II_D2.2-report_2016.02.15.pdf.
[30] Certaines autorités de protection fournissent néanmoins des statistiques annuellement ou lors de conférence. Ainsi l'autorité néerlandaise vient d'annoncer qu'elle a reçu 155 demande en matière de droit à l'oubli et a obtenu une médiation dans une cinquante de cas. Le rapport annuel 2016 de la CNIL fait état de 1000 demandes reçues depuis mai 2014, cf p.59. De son côté l'autorité de protection anglaise, l'ICO donne sur son site des chiffres anciens d'août 2015. https://iconewsblog.wordpress.com/2015/11/02/has-the-search-result-ruling-stopped-the-internet-working/
[31] Guidelines on the implementation of the Court of Justice of the European Union judgment on « Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzalez » C-131/12, 26 nov. 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf
[32] Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain adopted on 16 December 2015, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf

à Google Spain, alors que la Chambre administrative considère que seul Google Inc. est concerné, (Miquel Perguera).

Les contributions attestent également de l'existence dans les cinq Etats étudiés (Espagne, Allemagne, France, Italie, Royaume-Uni, Suède) de premières décisions juridictionnelles relatives à la mise en oeuvre du droit au déréférencement. Cela dit, au Royaume-Uni les affaires ont toutes conduites à un règlement à l'amiable, (David Erdos). Dans chaque pays étudié, les affaires juridictionnelles traitent des difficultés posées par les archives en ligne des journaux, qui permettent de retrouver de façon perenne des informations sur l'histoire des personnes concernées. Certaines affaires illustrent comment la notion de figure publique a été interprétée par le juge pour refuser le droit au déréférencement (Patricia Jonason). Certaines décisions juridictionnelles témoignent du développement d'obligations particulières pour les organismes de presse en ligne venant compléter le droit des personnes concernées. Ainsi la Cour Suprême espagnole dans un arrêt du 15 ocotbre 2015 prône l'usage de robots.txt de manière à rendre inaccessibles les données personnelles dans ces archives, (Miguel Perguera). La Cour Surpême italienne dans un arrêt de 2012 antérieur à l'arrêt Google avait déjà considéré que les organes de presse en ligne avaient une obligation de mise à jour de leur contenu. Dans un arrêt du 3 décembre 2015, elle semble aller jusqu'à reconnaître la possibilité que les nouvelles journalistiques aient une date limite de péremption, ce qui a fait l'objet de sevères critiques. (Giulia Tiberi). Au final, ces affaires attestent que le régime du traitement des données sensibles et des données relatives aux infractions pénales par les organes de presse en ligne constituent l'une des difficultés majeures sur laquelle la CJUE sera amenée aussi à se prononcer en raison d'une question préjudicielle du Conseil d'Etat français (Olivia Tambou, Giulia Tiberi). L'ensemble des contributions illustrent ainsi des difficultés dans la réalisation concrète de la mise en balance de l'intérêt du public à connaître l'information en cause avec les droits et libertés des personnes concernées.

Au delà des juges, le traitement du droit au déréférencement par les autorités nationales de protection témoignent également de disparités nationales. Les autorités étudiées informent les personnes concernées sur ce nouveau droit, certaines ont adopté un formulaire pour recevoir les plaintes en la matière. La CNIL en France[32], *l'Information Commissioner's Office* au Royaume-Uni (David Erdos) se contentent d'évoquer sous forme de statistiques le traitement du droit au déréférencement dans leur rapport annuel. Seule la *Datainspektion* suédoise a renseigné de manière très précise et transparente la mission d'inspection qu'elle a mise en place auprès de Google sur la base d'une sélection de treize plaintes. Cette transparence cache néanmoins l'actuelle limite du système de contrôle par l'autorité de protection suèdoise qui n'est pas obligée de donner suite à une plainte. Cela montre l'intérêt de l'harmonisation des missions, compétences et pouvoirs des autorités nationales de protection réalisée par le RGPD. (Patrica Jonason).

B- La valeur ajoutée de la reconnaissance d'un droit à l'oubli numérique

Face aux critiques bien connues sur le droit à l'oubli, Paul Bernal soutient que ce droit renforce la liberté d'expression et l'accès à l'information. Le droit à l'oubli contribue à faire remonter les articles les plus pertinents dans un moteur de recherche. Ainsi, le droit à l'oubli est un moyen d'équilibrer la faiblesse intrinsèque des algorithmes qui tendent à donner la priorité à ce qui est populaire plutôt qu'à ce qui est important. Il peut constituer une limite à l'instrumentalisation des moteurs de recherche pour véhiculer de fausses informations. Les critiques actuelles liées à la régulation privée par Google de ce droit invitent Nicolas Zingales et Agnieszka Janczuk-Gorywoda à proposer un autre modèle de co-régulation. Ce dernier reposerait sur la création d'une agence pour la liberté d'expression et d'information. Il serait complété par des principes notamment celui de la participation de l'ensemble des acteurs. Il reposerait également sur un processus de décision transparent et ouvert.

D'autres contributions questionnent la valeur ajoutée de l'introduction d'un droit à l'oubli numérique dans le RGPD. Pieter Van Cleynenbreugel relève l'ambiguïté actuelle de l'article 17 du RGPD qui ne permet pas de dire clairement ce qui doit être oublié. Ce droit ouvre-t-il simplement un droit au déréfencement de données personnelles ou comprend t-il une véritable suppression des données concernées. Cette ambiguité doit être clarifiée afin de comprendre comment les responsables de données doivent pouvoir se conformer à ce nouveau droit à l'oubli numérique. Olivia Tambou, rappelle que cette ambiguïté textuelle traduit en réalité un compromis politique entre le Parlement européen et le Conseil lors de l'adoption de l'article 17 RGPD. Selon elle,

[32] La CNIL rappelle dans son rapport 2017 qu'elle a été saisie de plus de 1000 demandes depuis mai 2014 en matière de déréférencement. cf. p. 61.

la valeur ajoutée de cette reconnaissance doit plutôt être analysée à l'aune des autres avancées du RGPD notamment la responsabilisation des acteurs sous le contrôle des autorités de protection des données dont les compétences sont harmonisées. Enrico Peucer se livre à une appréciation très critique de la reconnaissance de ce droit à l'oubli numérique. Il fait également état de la loi allemande d'adaptation au RGPD. Il souligne que son §35 autorise des restrictions au droit d'effacement ce qui comprend le volet du droit à l'oubli numérique.

C- L'absence de réelles alternatives trouvées hors Europe à la reconnaissance d'un droit à l'oubli numérique

Si la Russie est l'un des rares pays à avoir consacré un droit à l'oubli[33], Cyril Cohendy montre que ce droit n'opère aucun équilibre entre la protection de la vie privée et l'intérêt du public à l'information, ni même l'intérêt économique du moteur de recherche. L'identité des termes masque des situations très différentes.

Au Canada, Pierre-Luc Deziel rappelle qu'il n'existe pas de droit à l'oubli tel que l'envisage l'Union européenne. Les juges peuvent néanmoins adopter des jugements déclaratoires constatant une violation de la loi relative à la protection des données . Ces jugements ont vocation à être utilisés par les personnes concernées pour inciter le moteur de recherche à opérer le déréférencement d'URLs.

En Argentine, Juan Gustavo Corvalan rappelle que les souvenirs de la dictature militaire expliquent largement l'absence de reconnaissance d'un droit à l'oubli. Il n'existe pas actuellement de cadre légal suffisant pour une telle consécration. Le déréférencement est envisagé sous l'angle de la responsabilité des moteurs de recherche. Dès lors, il ne concerne que les contenus illicites. En effet, la Cour Suprême dans son arrêt *Rodriguez* a consacré la responsabilité limitée des moteurs de recherche à raison des contenus qu'ils diffusent. Le déréférencement repose sur l'existence d'une illégalité qui doit être notifiée au moteur de recherche. En cas de litige sur l'existence d'une illégalité, le juge sera le seul compétent pour ordonner le déréférencement.

Rafael Valim et Silvio Luis Ferreira Da Rocha montrent que la jurisprudence brésilienne se réfère à l'arrêt *Google Spain*, mais elle considère qu'elle ne peut pas imposer à un tiers, qui n'est pas le propriétaire de l'information, la fonction de retirer l'accès au grand public d'un ensemble de données déterminées.

Au Chili, Pedro Anguita Ramirez souligne que le droit à l'oubli a été envisagé dans le cadre de recours devant les tribunaux portant sur des demandes d'indemnisation en raison de violations du respect de la vie privée et du droit à l'honneur. Le droit à l'oubli a été au coeur de l'arrêt de la Cour Suprême *Graziani* où une personne jugée pour des crimes sexuels sur mineurs a obtenu la suppression d'un article relatant ces faits datant de onze ans dans les archives d'un journal en ligne. L'auteur interroge néanmoins la compatibilité de cette solution au regard de la liberté d'expression, telle qu'elle est consacrée à l'article 13 de la Convention américaine relative aux droits de l'Homme.

Au Mexique, Olivia Andréa Mendoza Enriquez rappelle que le déréférencement de liens sans pour autant effacer l'information sur la source originale constitue une censure selon l'autorité nationale chargée de la protection des données (INAI). A défaut de droit à l'oubli, la diffusion d'information erronée ou incorrecte peut être condamnée soit sur la base du droit à l'image, ou d'un droit de réponse, ou des actions en responsabilité civile.

Au Japon, le professeur Shizuo Fujiwara fait état de l'arrêt de la Cour Suprême du 31 janvier 2017 qui ne parle pas explicitement de droit à l'oubli. Il considère qu'il n'existe pas en soi de droit à l'oubli autonome, mais simplement un droit de demander une injonction pour retirer des liens sur la base d'une violation du droit à l'honneur et/ou du respect à la vie privée.

Hsu Pia Hao relate une difficulté particulière ayant conduit au rejet de demandes déréférencement par des résidents taiwanais. En effet, contrairement à ce qu'a jugé la CJUE dans son arrêt *Google Spain*, les tribunaux taiwanais n'ont pas reconnu l'existence d'une unité entre la société Google Inc. et sa filiale locale. L'auteur évoque aussi une affaire concernant une demande de déréférencement en Chine auprès du moteur de recherche Baidu. En l'espèce, la requête a été rejetée sur la base d'une absence d'atteinte à la réputation et au nom de la personne concernée. La juridiction s'est clairement prononcée sur l'absence d'un droit à l'oubli numérique en droit chinois.

[33] La Turquie a établi sa propre version d'un droit à l'oubli en octobre 2016. cf. Begüm Yavuzdoğan Okumuş and Bensu Aydin, Turkey's Court of Constitution Officially Recognizes Right to be Forgotten, IAPP Privacy Tracker, in 12.10.2016.

Partie 1 : La mise en œuvre nationale de l'arrêt Google Spain
Part 1: The domestic implementation of the Google Spain Case

THE APPLICATION OF THE RIGHT TO BE FORGOTTEN IN SPAIN

By Miquel Peguera
Associate Professor of Law at Universitat Oberta de Catalunya (UOC) (Barcelona, Spain).

This brief contribution summarises the main trends in the application of the right to be forgotten by courts and the Data Protection Authority in Spain. Courts' rulings and DPA's decisions are based on a case-by-case analysis of the facts, to determine whether the right of the data subject must prevail. While some criteria appear to be settled by now, some seem to be still tentative, and a fair amount of uncertainty remains.

Spain is an interesting country when it comes to the so-called 'right to be forgotten' (RTBF). After all, the famous CJEU judgment[1] recognizing this right in relation to search engines stemmed from a request for a preliminary ruling made by a Spanish court (the Audiencia Nacional, AN) following a procedure initiated before the Spanish Data Protection Authority (DPA) by a Barcelona citizen, Mario Costeja González. Likewise, the reasoning which was eventually endorsed by the CJEU – though with a slightly different reach – was a construction put forward by the Spanish DPA.

Now that amost four years have passed since the ruling was handed down, Google reports it has received requests to delist more than 203 543 URLs by individuals related to Spain, which makes it the fourth EU country by number of requests.[2] More than 64,945 URLs – around 38 % of all of those which have been already fully processed – have been delisted by Google.

Interestingly, courts and the DPA have issued a fair amount of decisions in Spain. The DPA has handed down more than five hundred decisions. Those typically arise from petitions by individuals whose removal requests were denied by Google or other search engines. Some of those decisions were subsequently appealed before the AN, which has delivered close to eighty rulings. In addition, a few cases brought directly before civil courts have also dealt with the right to be forgotten.

Some of the most interesting aspects of the way the right is being implemented in Spain may be summarized as follows:

I-THE STANDING OF THE SPANISH SUBSIDIARY.

Most of the cases that were pending before the AN when it made the referral to the CJEU were directed against the Spanish subsidiary of Google Inc (Google Spain, SL). In a dramatic move, some sixty AN judgments were reversed and voided by the Administrative Chamber of the Supreme Court on the grounds that Google Spain SL lacks standing to be sued, as the actual controller is only the American company. Unfortunately, the Supreme Court did not deal with the underlying merits of the cases, and thus the value of the material criteria articulated by the AN in all those rulings remains uncertain. More strikingly, a different Chamber of the Supreme Court – the Civil one – disagrees with the Administrative Chamber, and holds that the Spanish subsidiary does have standing.[3]

II-GEO-BLOCKING.

The Spanish DPA considers that the delisting from the European domains of Google is not enough to fully comply with the CJEU judgment, as any user located

1 CJEU, judgment of 13 May 2014, Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] <http://curia.europa.eu/juris/liste.jsf?num=C-131/12>.

2 Google, 'Search Removals under European Privacy Law' (Transparency Report) <https://transparencyreport.google.com/eu-privacy/overview>.

3 M Peguera, 'Clash between Different Chambers of the Spanish Supreme Court on the Right to be Forgotten' (ISP Liability, 11 April 2016) <https://ispliability.wordpress.com/2016/04/11/clash_between_different_chambers/>.

THE RIGHT TO BE FORGOTTEN IN SPAIN

in Spain could easily resort to the Google.com version to find the delisted link. However, the DPA appears to accept that geo-blocking would be enough, that is, blocking the access to the link in any domain, when the search is carried out by someone from a computer located in Spain.[4]

III-COMMUNICATION WITH THE PUBLISHER.

Once the search engine has decided to delist a link to a piece of content, may Google inform the publisher about the delisting – a usual practice when the webmaster has registered with the tool called "search console"? The Spanish DPA found that it can't, and fined Google for such a communication,[5] holding that it violates the duty of secrecy set forth in the Data Protection Act.[6] The decision is under appeal.

IV-INDIVIDUALS WITH NO RELATIONSHIP TO THE EU.

Data subjects requesting URLs removals must bear some link to EU countries. In several decisions, the DPA has rejected requests from data subjects residing in Latin American countries, noting that the individuals had no meaningful link with the EU territory.[7]

V-ARE HOSTS ALSO CONTROLLERS?

The Costeja case related to search engines, and concluded that they are controllers of the personal data shown in the results and in the content to which they link. May the same conclusion be held for providers of hosting services, though they are arguably in a very different situation? The Spanish DPA – following the AN's criteria – considers that a hosting platform such as Blogger is not a data controller. However, it deems YouTube a data controller,[8] though holding at the same time that it may rely on the hosting safe harbour provided by the eCommerce Directive.[9] In this vein, the DPA holds that while YouTube is not liable for the challenged content, it must remove it once it is notified of its illegal nature by a competent authority – such as the DPA itself.

VI-DAMAGES FOR FAILING TO DELIST.

In a civil lawsuit, finally decided by the Supreme Court, Google was ordered to pay damages to the claimant for failing to remove a link to a notice of pardon published on the Official Gazette,[10] which revealed an old crime committed by the data subject.

VII-FURTHER REMOVAL DENIED FOR MR. COSTEJA.

The now famous lawyer requested the delisting of a blog post criticizing him. The DPA rejected,[11] noting that the facts of the Costeja case have now become a matter of public interest – and moreover he had granted multiple interviews in the media, thus allowing public discussion on the case.

VIII-BURDEN OF PROOF IN RELATION TO DATA ACCURACY.

When the accuracy of the data is challenged, decisions by the DPA are not fully consistent as to whether it is

4 Agencia Española de Protección de Datos, Decision of 2 December 2015 (TD/00930/2015) <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2015/common/pdfs/TD-00930-2015_Resolucion-de-fecha-02-12-2015_Art-ii-culo-16-LOPD.pdf>.

5 D Erdos, 'Communicating Responsibilities: The Spanish DPA Targets Google's Notification Practices when Delisting Personal Information' (The International Forum for Responsible Media Blog, 31 March 2017) <https://inforrm.org/2017/03/21/communicating-responsibilities-the-spanish-dpa-targets-googles-notification-practices-when-delisting-personal-information-david-erdos/>.

6 M Peguera, 'Derecho al olvido: ¿el buscador puede informar a la fuente de la eliminación de un enlace?' (Responsabilidad en Internet, 4 March 2017) <https://responsabilidadinternet.wordpress.com/2017/03/04/derecho-al-olvido-el-buscador-puede-informar-a-la-fuente-de-la-eliminacion-de-un-enlace/>.

7 Agencia Española de Protección de Datos, Decision of 31 March 2015 (TD/01094/2014) <http://www.agpd.es/portalwebAGPD/resoluciones/recursos_reposicion/rr_sobre_tutela_de_derechos/common/pdfs/REPOSICION-TD-01094-2014_Resolucion-de-fecha-31-03-2015_Art-ii-culo-34-RD-1720-b-2007.pdf>; Agencia Española de Protección de Datos, Decision of 11 December 2015 (TD/01172/2015) <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2015/common/pdfs/TD-01172-2015_Resolucion-de-fecha-11-12-2015_Art-ii-culo-16-LOPD_Recurrida.pdf>.

8 Agencia Española de Protección de Datos, Decision of 5 October 2016 (TD/00799/2016) <http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2016/common/pdfs/TD-00799-2016_Resolucion-de-fecha-05-10-2016_Art-ii-culo-16-LOPD.pdf >.

9 Council Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L178/1 <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32000L0031>.

10 M Peguera, 'Right to be Forgotten: Google Sentenced to Pay Damages in Spain' (The Centre for Internet and Society, Stanford Law School, 14 October 2014) <https://cyberlaw.stanford.edu/blog/2014/10/right-be-forgotten-google-sentenced-pay-damages-spain>.

11 M Peguera, 'No More Right-To-Be-Forgotten for Mr Costeja, Says Spanish Data Protection Authority' (The Centre for Internet and Society, Stanford Law School, 3 October 2015) <https://cyberlaw.stanford.edu/blog/2015/10/no-more-right-be-forgotten-mr-costeja-says-spanish-data-protection-authority>.

THE RIGHT TO BE FORGOTTEN IN SPAIN

the data subject who must prove the inaccuracy, or if it is the search engine that must prove the accuracy to be able to reject the delisting request.

IX-EXCLUSION PROTOCOLS.

The Supreme Court has held that while an individual has no right to supress content from a newspaper's historic archive, the publisher must implement exclusion protocols such as robots.txt or metatags so that the content is not indexed by search engines.[12] Failing to do so amounts to an illegal processing by the publisher.

X-WEBSITES' INTERNAL SEARCH TOOLS.

While a data subject may obtain the delisting from search engines, requests that the links are also delisted from the internal search tools of a website – such as that of a newspaper – are rejected, on the grounds that this would affect freedom of expression.[13]

XI-SOME GROUNDS FOR DENYING RTBF REQUESTS.

The DPA issued a decision granting the delisting in relation to negative comments about the professional conduct of a medical doctor. Nonetheless, the Audiencia Nacional reversed that decision in May 2017,[14] noting that in that case the interests of the public must prevail, as current and prospective patients of that doctor have the right to know about the experiences and opinions expressed by former patients. Similarly, the Audiencia Nacional, in June 2017, reversed a DPA decision regarding electoral information.[15] The AN held that the list of the candidates of a 2011 municipal election is still of public interest, which must prevail over the interest of the data subject who requests the delisting.

To conclude, while RTBF requests are decided on a case by case basis, in most cases both the DPA and the courts offer little justification on why a particular case deserves the requested delisting or not – beyond the most obvious situations involving public figures–, and thus legal certainty is still far from being achieved.

12 Spanish Supreme Court, Civil Chamber, judgment of 15 October 2015 (ECLI: ES:TS:2015:4132), <http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=7494889&links=2807911991201510003 4&optimize=20151019&publicinterface=true>.
13 Id.
14 Audiencia Nacional, judgment of 11 May 2017 (ECLI: ES-:AN:2017:2433) <http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=8095052&links=&optimize=20170713&publicinterface=true>.
15 Audiencia Nacional, judgment of 19 June 2017 (ECLI: ES-:AN:2017:2562) <http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=8104123&links=&optimize=20170720&publicinterface=true>.

THE "RIGHT TO BE FORGOTTEN" IN GERMANY

By Dr. Enrico Peuker
Post-Doc at Humboldt-University of Berlin

This article gives a brief introduction to the merits and misunderstandings of the ECJ's *Google Spain* ruling and its reception by German courts. It further analyses the "right to be forgotten" in the context of the new European General Data Protection Regulation and the German implementation Act referring to this. The article concludes with the recommendation to abstain from the notion of "right to be forgotten" being a buzzword in the recent discussion about (European) data protection law.

The "right to be forgotten" is a buzzword in the recent discussion about data protection law.[1] Originally a literary idea, an elaborated concept with anthropological, psychological and social connotations,[2] it inevitably shared the same fate as other buzzwords: quickly wrested from its original context, it became independent and thereby lost its distinctive character. As a little meaningful term, it invited misunderstandings and misinterpretations. So, it is not astonishing that the right to be forgotten attracted attention from politics, the media and legal scholarship – not only in the context of the European Court of Justice's (ECJ) *Google Spain* ruling,[3] but also during and after the passing of the European General Data Protection Regulation whose Art. 17 is accordingly headlined.

As a consequence of this "buzzword fate", the right to be forgotten does not suffice for a legal term. Accordingly, the reactions in German legal discussion have been rather reserved, not at least proven by the fact that the "right to be forgotten" is always referred to in quotation marks. This article intends to give a brief introduction to the merits and misunderstandings of the ECJ's *Google Spain* ruling and its reception by German courts. It further analyses the "right to be forgotten" in the context of the new European General Data Protection Regulation and the German implementation act referring to this, both applicable from May 2018. The article concludes with the recommendation to abstain from the notion of "right to be forgotten".

I-THE *GOOGLE SPAIN* RULING

A-Merits and Misunderstandings

The ECJ's *Google Spain* ruling deserves attention for several reasons. First, the ECJ demonstrates its pretensions to be an effective fundamental rights protector in the European Union against earlier criticism. Second, it highlights the constitutional or fundamental rights basis of European data protection law in Art. 7 and 8 of the Charter of Fundamental Rights of the European Union (CFR) taking up the judicature it started with the *Schecke & Eifert*-case.[4] In fact, *Google Spain* was the starting point of a number of spectacular decisions, where the ECJ annulled secondary law, for privacy and data protection reasons, or interpreted it in a data protection friendly way.[5] Third, the Court "extended" the territorial scope of the European Data Protection Directive. Finally, it clarified the data protection responsibility of the operator of the search engine that can be distinguished from, and

1 The author would like to thank Louise Majetschak, Moritz Schramm, Jasper Kamradt (Humboldt-University of Berlin), and Sam Bourton (UWE Bristol) for proofreading.
2 Viktor Mayer-Schönberger, Delete. Die Tugend des Vergessens im digitalen Zeitalter (Berlin University Press 2010) 199 et seq; see also Bert-Jaap Koops, 'Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right to be Forgotten" in Big Data Practice' (2011) 8 SCRIPTed 229, 231 et seq.
3 Case C-131/12 *Google Spain SL v AEPD* (2014) ECLI:EU:C:2014:317.
4 Cases C-92/09 and 93/09 *Schecke & Eifert v Land Hessen* (2010) ECLI:EU:C:2010:662.
5 Case C-293/12 *Digital Rights Ireland* (2014) ECLI:EU:C:2014:238; case C-362/14 *Schrems* (2015) ECLI:EU:C:2015:650.

THE RIGHT TO BE FORGOTTEN IN GERMANY

is additional to, that of publishers of websites who load personal data on a webpage.[6] These reasons qualify the *Google Spain* ruling as a landmark decision.

However, although argued for,[7] the ECJ has not developed Art. 7 and 8 CFR into an autonomous "fundamental right to be forgotten in the internet".[8] Due to the nature of a preliminary ruling proceeding, the ECJ did not invent new fundamental rights, but interpreted acts of the EU institutions, i.e. secondary EU law, according to Art. 267 lit. b TFEU, nevertheless in the light of fundamental rights. The *Google Spain* ruling deals with the interpretation of Art. 12 lit. b of the 1995 EC Data Protection Directive[9]. This provision contains the well-known data subject's right to erasure of unlawfully processed data that is also provided in many other international and domestic data protection acts.[10] The Court consequently did not pick up the term "right to be forgotten" that has been pleaded by the parties of the preliminary ruling procedure.[11] Instead, it interpreted Art. 12 lit. b of the Directive as meaning that the operator of a search engine is obliged to remove listings from the list of results if (1.) they follow a search made on the basis of a person's name, and (2.) contain links to web pages that are published by third parties and contain information relating to that person.[12] Therefore, not a fundamental right to be forgotten, but rather the data subject's[13] right to erasure obliges the operator of a search engine not to display the data subject's personal data in a list of results if this data processing is unlawful.[14] In the case at hand, the data processing was unlawful because there were no particular reasons substantiating a preponderant interest of the public in having access to the privacy-sensitive information that a person has been involved in a real-estate auction connected with attachment proceedings for the recovery of social security debts 16 years ago.

B-German Case Law after *Google Spain*

So far, German courts have not directly applied the 1995 EC Data Protection Directive in data protection cases, but the German implementation act to this directive, the so called "Bundesdatenschutzgesetz" (BDSG).[15] The first version of the BDSG was passed in 1977 as one of the first data protection laws worldwide[16] and was reformed several times, in order to implement the requirements of the EC Data Protection Directive. Thus, German courts apply German data protection law in the light of the EC directive that is interpreted by the

6 The ECJ justified the data protection responsibility of the operator of a search engine with the fact that data processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet – information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty – and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous (case C-131/12 *Google Spain SL v AEPD* (2014) ECLI:EU:C:2014:317, para 80).

7 Volker Boehme-Neßler, 'Das Recht auf Vergessenwerden – Ein neues Internet Grundrecht im Europäischen Recht' (2014) Neue Zeitschrift für Verwaltungsrecht 825.

8 Correctly seen by Norbert Nolte, 'Das Recht auf Vergessenwerden – Mehr als nur ein Hype?' (2014) Neue Juristische Wochenschrift 2238.

9 Data Protection Directive 95/46/EC (1995) OJ L281/31.

10 For instance Art. 8 lit. c of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention Nr. 108); No. 13 lit. d of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79. For the little relevance of international organization's data protection rules see Friederike Voskamp, Transnationaler Datenschutz. Globale Datenschutzstandards durch Selbstregulierung, (Nomos 2015) 26 et seq; Gabriela Zanfir, 'Tracing the Right to Be Forgotten in the Short History of Data Protection Law: The "New Clothes" of an Old Right' Forgotten' in: Serge Gutwirth and Ronald Leenes and Paul de Hert (eds), *Reforming European Data Protection Law* (Springer 2013) 227, 239 et seq.

11 Case C-131/12 Google Spain SL v AEPD (2014) ECLI:EU:C:2014:317, para 91.

12 Case C-131/12 Google Spain SL v AEPD (2014) ECLI:EU:C:2014:317, para 88.

13 Art. 4 no. 1 GDPR contains the legal definition of „data subject": that is a natural person identified or identifiable by personal data. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

14 Anika D. Luch and Söhnke E. Schulz and Florian Kuhlmann, 'Ein Recht auf Vergessenwerden als Ausprägung einer selbstbestimmten digitalen Persönlichkeit. Anmerkung zum Urteil des EuGH v. 13.5.2014 (Google), Rs. C-131/12' (2014) Europarecht 698, 704; Oskar Josef Gstrein, Das Recht auf Vergessenwerden als Menschenrecht. Hat Menschenwürde im Informationszeitalter eine Zukunft? (Nomos 2016) 107 et seq.

15 And the case may be – due to German federalism – more specific German data protection acts on the federal or the federal states' level.

16 The first data protection act of the world was the Data Protection Act of the German federal state Hesse in 1970.

THE RIGHT TO BE FORGOTTEN IN GERMANY

ECJ in cases such as *Google Spain*. However, there are only a few judgements of German courts referring to the ECJ's *Google Spain* ruling, and most of them deal with aspects of data protection responsibility,[17] the competence of a Member State's supervisory authority[18] or the notion of an establishment.[19]

The case of the Higher Regional Court of Cologne, concerning listings in a search engine's list of results, is the only case where the "right to be forgotten" and the *Google Spain* ruling are a central theme.[20] The plaintiff was a former director of an enterprise (5 years prior to the judgment), which ran an online dating website. The name of the plaintiff as a director can be seen on websites with former extracts of the commercial register as well as in anonymous online blog posts decrying unfair business practices of the said enterprise. Thus, the plaintiff filed an action for an injunction against the operator of the search engine to prevent it from displaying links to these websites and blog posts in the list of results. First of all, the court stated – based on domestic data protection and civil law – that the plaintiff has no right to omission or erasure concerning the listings in the list of results, because there had been no infringement of her personal rights.

The fact that she was a former director of an enterprise is – as a true matter of fact – an issue of a person's so called "social sphere" in which an infringement of personal rights can only be possible in cases of severe effects on one's personality, such as stigmatisation, social marginalisation or pillory effects.[21]

But this was not the case at bar: with regard to the plaintiff's former position as a director as a matter of the "social sphere", her right to data protection does not prevail over the freedom of information of the search engine users/the public as well as the freedom of expression of the blog post authors.[22] Furthermore, the court did not see the need for a modification of German civil law's criteria in the light of the *Google Spain* ruling, because both cases were to be distinguished[23]: On the one hand, the plaintiff's case did not concern information which was 16 years old, but merely 5. On the other hand, the true and objective information about the plaintiff's position is not as privacy-sensitive as the fact that a person – as in *Google Spain* – had been involved in a real-estate auction connected with attachment proceedings for the recovery of social security debts. In addition, the information in question in the German case arose from a public commercial register. And finally, since the online dating website is still running and still incriminated for unfair business practices, there is a countervailing public interest to information about the person, who was until not so long ago responsible for those business practices.

Although up until now the case of the Higher Regional Court of Cologne is the only one dealing with the ECJ's *Google Spain* ruling from a German court perspective on the Higher Regional Courts level, it seems to exemplify a possible strategy of handling the ECJ's *Google Spain* ruling. German courts may fit the *Google Spain* ruling into the elaborated German concept of personal rights protection[24] and in doing so, respect the ECJ's legal assessments with regard to the "right to be forgotten" while interpreting and applying German data protection and civil law.[25] Nevertheless, contrary to what the ECJ

17 1) In the case of the Higher Adminstrative Court (Oberverwaltungsgericht) of Schleswig-Holstein, ECLI:DE:OVGSH:2014:0904.4LB20.13.0A, the court declined the data protection responsibility of the operator of a Facebook Fanpage as well as a common data protection responsibility of this operator and Facebook because this case is different from Google Spain ruling. Currently, the case is under appeal at the Federal Administrative Court (Bundesverwaltungsgericht), that has requested a preliminary ruling by the ECJ (C-210/16) – ECLI:DE:BVerwG:2016:250216B1C28.14.0.
2) In the case of the Regional Court (Landgericht) Berlin, ECLI:DE:LGBE:2014:0821.270293.14.0A, the court pointed out that there is no data protection responsibility by a German subsidiary of Google Inc., that does not offer a search engine service, but only by Google Inc. The Regional Court (Landgericht) Hamburg, ECLI:DE:LGHH:2016:0129.3240456.14.0A, concurred in the Regional Court Berlin's legal opinion.

18 In the case of the Higher Administrative Court (Oberverwaltungsgericht) of Hamburg, ECLI:DE:OVGHH:2016:0629.5BS40.16.0A, the court raised but did not answer the question whether a German supervisory authority can proceed against the Irish subsidiary of Facebook because of the duty to use 'real names' on Facebook.

19 Request for a preliminary ruling by the Higher Regional Court (Oberlandesgericht) Düsseldorf in a trademark law case, I-20 U 68/15, 20 U 68/15.

20 Higher Regional Court (Oberlandesgericht) Köln, I-15 U 197/15, 15 U 197/15. The right to be forgotten is not mentioned explicitly in the case of Regional Court (Landgericht) Ham-burg, ECLI:DE:LGHH:2016:0129.3240456.14.0A. Nevertheless, the court did a proportionate balanc-ing of the opposing fundamental rights and interests in the light of the German "sphere concept" of per-sonal rights protection explained in the following footnote.

21 German case law on the protection of personal rights distinguishes between three spheres – the private sphere, the personal sphere and social sphere – in which personal data is protected to a different extent. Meaning that the requirements for a justification of infringements increase on every stage of this sphere concept from social to private sphere.

22 Higher Regional Court (Oberlandesgericht) Köln, I-15 U 197/15, 15 U 197/15, para 59 et seq.

23 Higher Regional Court (Oberlandesgericht) Köln, I-15 U 197/15, 15 U 197/15, para 67 et seq.

24 See Fn. 18.

25 As the Regional Court (Landgericht) Hamburg did in the case ECLI:DE:LGHH:2016:0129.3240456.14.0A.

seems to suggest in *Google Spain*,[26] one cannot state a general priority of the data protection right over third parties' fundamental rights or public interests. Rather, it depends on a proportionate balancing of the opposing fundamental rights and interests in each case.[27]

II-THE "RIGHT TO BE FORGOTTEN" IN THE EU GENERAL DATA PROTECTION REGULATION

The "right to be forgotten" was also a central issue in the reform of European data protection law.[28] With this reform, the European Commission tended to strengthen the rights of individuals conceptualised as data subjects. Regarding individual rights, the Commission pointed to three main shortcomings as a cause for the reform: an insufficient harmonization of national data protection laws dealing with individual rights, insufficient powers of national authorities to ensure an effective exercise of individual rights, and an insufficient awareness of individuals about their rights in data processing. This was deemed to be especially prevalent in online data processing. Thus, the Commission aimed at giving people efficient and operational means to ensure that they are fully informed about what happens to their personal data, enabling them to exercise their rights more effectively.

As the result of a four year legislative process, the European Parliament and the Council enacted the European General Data Protection Regulation (GDPR) in April 2016 which shall apply from May 2018. The notion of the "right to be forgotten" headlines Art. 17 GDPR in quotation marks and brackets beside the term "right to erasure" – although this notion has already been criticised as unnecessary, confusing, delusive and even as a bluff package not only by German legal scholarship.[29] The use of quotation marks in the headline of Art. 17 may indicate the EU legislator's own doubts concerning the notions validity.

Since para. 1 of Art. 17 deals with the right to erasure (that has already been provided in the 1995 EC Data Protection Directive) and para. 3 sets exceptions to the right to erasure, the "right to be forgotten" must be hidden in para. 2. According to para. 2, the controller[30] shall take reasonable steps to inform third controllers who 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, where he has made the personal data public and is obliged to erase the personal data. Para. 2 addresses the internet-typical problem that any person can adopt and process information published on the internet. However, Art. 17 only obliges the controller to inform third controllers about the data subject's request for erasure, thereby taking into account available technology and the cost of implementation. Distinct from the proposal of the European Parliament, the controller is not obliged to ensure that third controllers erase the data (so called *obligation de moyens*). Thus, Art. 17 para. 2 seems to be a very poor implementation of a "right to be forgotten" – no erasure, but the mere information/notification of third controllers. In addition, the legal and factual consequences of Art. 17 para. 2 are actually far from clear. First of all, it could be impossible to determine all third parties who have processed data published on the internet. Then, it is questionable whether the information about a data subject's request for erasure

26 Case C-131/12 Google Spain SL v AEPD (2014) ECLI:EU:C:2014:317, para 81: „Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users […]".

27 Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015) 147 et seq; Jürgen Kühling, 'Rückkehr des Rechts: Verpflichtung von „Google & Co." zu Datenschutz' (2014) Europäische Zeitschrift für Wirtschaftsrecht 527, 529; Johannes Masing, 'Vorläufige Einschätzung der „Google-Entscheidung" des EuGH' (Verfassungsblog, 14 August 2014) <http://verfassungsblog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh/> accessed on 10 October 2017; Herke Kranenborg, 'Google and the Right to Be Forgotten (Case C-131/12, Google Spain)' (2015) 1 European Data Protection Law Review 70, 74; Maximilian von Grafenstein and Wolfgang Schulz, 'The right to be forgotten in data protection law: a search for the concept of protection' (2016) 5 International Journal of Public Law and Policy 249, 262 et seq.

28 Cf. the former European Commissioner for Justice, Fundamental Rights and Citizenship Viviane Reding, 'The EU Data Protection Reform: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age' Speech 12/26, 5; Viviane Reding, 'The European data protection framework for the twenty-first century' (2012) International Data Privacy Law 119, 125.

29 Ansgar Koreng and Thorsten Feldmann, 'Das „Recht auf Vergessen". Überlegungen zum Konflikt zwischen Datenschutz und Meinungsfreiheit' (2012) Zeitschrift für Datenschutz 311, 315; Gerrit Hornung and Kai Hofmann, 'Ein "Recht auf Vergessenwerden"?' (2013) Juristenzeitung 163, 170; Jürgen Kühling, 'Rückkehr des Rechts: Verpflichtung von „Google & Co." zu Datenschutz' (2014) Europäische Zeitschrift für Wirtschaftsrecht 527, 530; Christina Markou, 'The 'Right to Be Forgotten': Ten Reasons Why It Should Be Forgotten' in: Serge Gutwirth and Ronald Leenes and Paul de Hert (eds), Reforming European Data Protection Law (Springer 2013) 203, 211 et seq; Paul Bernal, 'The EU, the US and Right to be Forgotten' in: Gutwirth and Ronald Leenes and Paul de Hert (eds), *Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges* (Spinger 2014) 61, 75 et seq; Alexander Roßnagel and Maxi Nebel and Philipp Richter, 'Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO' (2015) Zeitschrift für Datenschutz 455, 458.

30 I.e. the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (Art. 4 no. 7 GDPR).

on the website of the controller constitutes a proactive informing of third controllers by the controller. Moreover, with regard to the available technology and the cost of implementation, it will often be impossible, or at least an unreasonable burden, for the controller to inform all third controllers.[31]

To conclude, there are a lot of good reasons to forgo the notion of "right to be forgotten" – not only in the context of the GDPR. If the right to be forgotten means nothing else than the well-known right to erasure, there is no need for introducing a synonym.[32] The duty to inform third controllers originating from para. 2 is only a humble contribution to achieving being forgotten. Moreover, the technical process of erasing data is exaggerated by describing it with the notion of "being forgotten" and its anthropological, psychological and social connotations. However, Art. 17 does not reflect the sophisticated concept of the "right to be forgotten" and its critique. Finally, the saying of *a right to* be forgotten seems to point to a concept of property rights on personal data - currently a highly controversially debated issue.[33] At least, it ignores the fact that one can hardly have a right against a third person to be forgotten by them.[34] So, if the notion of the "right to be forgotten" is nothing else than the right to erasure of unlawfully processed personal data, the notion may have a heuristic function – if at all –, but is no good as a legal term.

III-THE GERMAN IMPLEMENTATION OF THE GDPR AND THE "RIGHT TO BE FORGOTTEN"

A-The Door Opener for Domestic Data Protection Restrictions

As stated in recital 10 of the GDPR, the level of protection of the rights and freedoms of natural persons with regard to the processing of personal data should be equivalent in all Member States in order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of such data within the EU. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. This pursued harmonisation of data protection law throughout the EU is exactly the reason why the EU legislator has chosen the regulation as a form of legislative action: the regulation shall have general application, shall be binding in its entirety and directly applicable in all Member States (Art. 288 TFEU) without any implementing acts that could lead to a different application of data protection law as well as legal uncertainty (as was the case under the 1995 Data Protection Directive regime).

However, according to Art. 23 GDPR, the rights of data subjects provided by the GDPR can be restricted by Member States (or Union) legislation, when such a restriction is a necessary and proportionate measure to safeguard private rights[35] and public interests.[3637] So the GDPR rather is a mixture of a regulation and a directive. This may have ensured the possibility of achieving consensus about the GDPR between the Member States. But Art. 23 relativizes the GDPR's harmonisation goal at the expense of legal certainty. Nevertheless, the harsh critique[38] of this door opener

31 See only Enrico Peuker, 'Kommentierung von Art. 17 DSGVO' in Gernot Sydow (ed), *Europäische Datenschutzgrundverordnung. Handkommentar* (Nomos 2017) para 51 et seq.
32 Other than Peter Schantz, 'Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht' (2016) Neue Juristische Wochenschrift 1841, 1845, who determines an upgrading of the right to erasure by a new notion.
33 Seminal Paul M. Schwartz, 'Property, Privacy, and Personal Data' (2004) 117 Harvard Law Review 2056, 2094 et seq; see further Nadezhda Purtova, Property Rights in Personal Data. A European Perspective (Kluwer Law International 2011) 91 et seq; Jacob M. Victor, 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy', (2013) 123 The Yale Law Journal 513, 516 et seq; for the German discussion see Thomas Hoeren, 'Dateneigentum – Versuch einer Anwendung von § 303a StGB im Zivilrecht' (2013) MultiMedia und Recht 486; Michael Dorner, 'Big Data und "Dateneigentum"' (2014) Computer und Recht 617, 618 et seq; Matthias Berberich and Sebastian J. Gola, 'Zur Konstruktion eines "Dateneigentums". Herleitung, Schutzrichtung, Abgrenzung' (2016) Privacy in Germany 165, 166 et seq.
34 Johannes Masing, 'Herausforderungen des Datenschutzes' (2012) Neue Juristische Wochenschrift 2305, 2307; Jef Ausloos, 'The 'Right to Be Forgotten' – Worth Remembering?' (2012) 28 Computer Law & Security Review 143, 144; Christina Markou, 'The 'Right to Be Forgotten': Ten Reasons Why It Should Be Forgotten' in: Serge Gutwirth and Ronald Leenes and Paul de Hert (eds), Reforming European Data Protection Law (Springer 2013) 203, 211 et seq.
35 For example the protection of the data subject or the rights and freedoms of others or the enforcement of civil law claims (Art. 23 para. 1 lit. i and j).
36 For example national security, defence, public security, the prosecution of criminal offences or the execution of criminal penalties or other important objectives of general public interest of the Union or of a Member State (cf. Art. 23 para. 1 lit. a-h).
37 Cf. Enrico Peuker, 'Kommentierung von Art. 23 DSGVO' in Gernot Sydow (ed), *Europäische Datenschutzgrundverordnung. Handkommentar* (Nomos 2017).
38 With regard to the precedent clause Ulrich Dammann and Spiros Simitis, EG-Datenschutzrichtlinie. Kommentar (Nomos 1997), Einleitung para. 37, 46: 'excessive accumulation of

clause has to take several points into account: Firstly, Art. 23 GDPR takes up the precedent provision in Art. 13 of the 1995 EC Data Protection Directive as well as the requirements of the CFR and the European Human Rights Convention in the interpretation by the ECJ and the European Court of Human Rights. Secondly, the allocation of competences between the EU and the Member States can explain some of the restriction goals in Art. 23 – the EU has no competence to regulate issues of national security for instance. Finally, the possible restrictions on data subjects' rights based on Art. 23 GDPR are restricted themselves by the essence of the fundamental rights and freedoms and the fact that they have to be a necessary and proportionate measure in a democratic society (Art. 23 para. 1).

B-The Reformed German Federal Data Protection Act of 2017

As one of the first EU Member States, Germany has passed an implementation act for the GDPR[39] that reforms the German Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) and enters into force in May 2018 – together with the application of the GDPR.[40] The implementation act fulfils Member States' regulatory obligations stated in the GDPR and makes use of some door opener clauses provided by the GDPR. The German government explicitly stated that they wanted to keep the existing German data protection rules under the GDPR regime as far as possible. The coexistence of European and domestic data protection rules makes the data protection law quite complex because the legal situation only arises when one reads both the GDPR and the domestic implementation or restriction norms together. And the fact that a domestic restriction of GDPR's clauses has to cite the GDPR clause does not really enhance the readability of these norms.

The German implementing legislator has passed some restrictions of data subject's rights based on Art. 23 GDPR. Restrictions on the right to erasure provided in Art. 17 GDPR are stated in § 35 BDSG. According to para. 1, there is no right to erasure, if – in cases of lawful non-automatic processing of personal data (i.e. paper-based archives or other analogue storage media) – the erasure would require an unreasonable effort and if the data subject has only a little interest in erasure. In this instance, a right to restriction of processing (Art. 18 GDPR[41]) supersedes the right to erasure. The same is true according to para. 2, if the controller may assume that the erasure would infringe the data subject's interests. Finally, according to para. 3, there is no right to erasure, but a right to restriction of processing, if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed but cannot be erased because of retention periods provided by statutes or contracts.

C-Legal Review of the Reformed 2017 Federal Data Protection Act

Since the reformed BDSG has not yet entered into force, there is no case law dealing with it. However, since the BDSG is one of the first Member State's implementation acts of the GDPR, the European Commission is likely to supervise the German implementation act and its application, especially with regard to the restriction of data subject's rights.[42]

IV-CONCLUSION

The "right to be forgotten" is a fancy buzzword, but not an elaborated legal concept. Beyond that, it has only little heuristic function unless it only refers to the wishful thinking that people shall forget some issues of a person's life. Thus, legal scholarship is well advised to concentrate less on the label of "the right to be forgotten" but rather on the interpretation of positive law (such as the GDPR, that unfortunately boosts the "right to be forgotten" by headlining Art. 17 with it). The same holds especially true for courts. German case law shows how to handle the ECJ's rulings by integrating them into an elaborate dogmatic concept without referring to a shapeless "right to be forgotten". In the end, the demand for concrete legal terms is not only an obsession of legal scholarship, but has two concrete reasons: On the one hand, concrete legal terms are the basis for supervisory authorities' action against

wilfully widely formulated general terms', 'dissimulation of data processing', 'lip service to fundamental rights based data protection.'

39 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 (DSGVO) und zur Umsetzung der Richtlinie (EU) 2016/680, Bundesgesetzblatt Jahrgang 2017, Teil I, Nr. 44, S. 2097.

40 For an overview Holger Greve, 'Das neue Bundesdatenschutzgesetz' (2017) Neue Zeitschrift für Verwaltungsrecht 737.

41 See Enrico Peuker, 'Kommentierung von Art. 18 DSGVO' in Gernot Sydow (ed), *Europäische Datenschutzgrundverordnung. Handkommentar* (Nomos 2017).

42 Cf. Holger Greve, 'Das neue Bundesdatenschutzgesetz' (2017) Neue Zeitschrift für Verwaltungsrecht 737 who reports about a possible infringement procedure against Germany.

THE RIGHT TO BE FORGOTTEN IN GERMANY

controllers. According to Art. 58 lit. para. 2 lit. g GDPR, the competent supervisory authority can order the erasure of personal data pursuant to Art. 17 para. 1 GDPR and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Art. 17 para. 2 GDPR. On the other hand, according to Art. 83 para. 5 lit. b GDPR, infringements of the data subject's right to erasure (or notification) can be subject to administrative fines up to 20.000.000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

TROIS ENSEIGNEMENTS À TIRER DE LA MISE EN OEUVRE JURIDICTIONNELLE FRANÇAISE DE L'ARRÊT GOOGLE SPAIN

par Olivia Tambou
Maître de Conférences HDR spécialisée en droit de l'Union européenne à l'Université Paris-Dauphine, PSL Research University, Cr2D

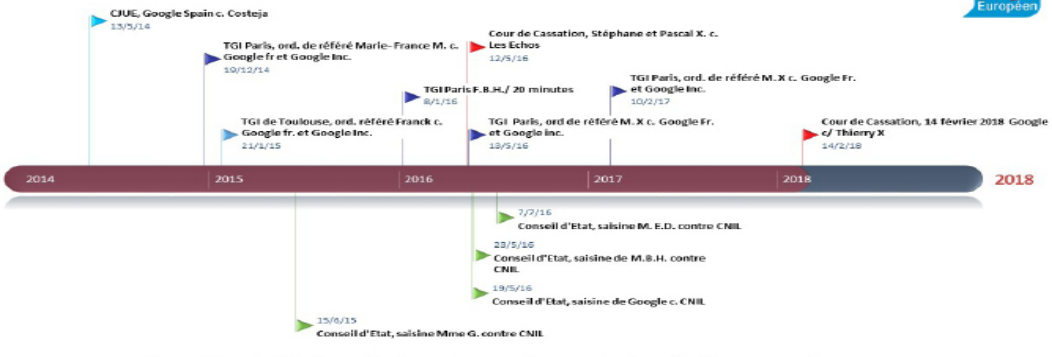
Il existe une dizaine de saisines de juges français relatives à la mise en oeuvre de l'arrêt Google Spain en France. La majorité sont des ordonnances de référés de TGI qui estiment que le refus de déréférencement demandé n'était pas justifié par le droit à l'information légitime du public. Le juge judiciaire considère également que ce droit ne s'impose pas aux organes de presse. Les requêtes portées contre les décisions de la CNIL devant le Conseil d'Etat attestent de la nécessité d'une clarification de la CJUE sur l'étendue des obligations des moteurs de recherche.

L'une des critiques faite à l'arrêt *Google Spain* est d'avoir érigé les moteurs de recherche, en juge du droit au déréférencement. Le fait que les moteurs de recherches en tant qu'intermédiaires techniques retirent des contenus sur Internet au nom du respect des droits d'auteurs n'a jamais choqué personne. Il est néanmoins en général opposé que, dans le cadre du droit au déréférencement, les enjeux seraient d'une toute autre importance. Il s'agit, en effet, de confier à une entreprise privée le soin d'exercer une balance des intérêts entre, d'une part, le droit à la protection des données personnelles des individus et, d'autre part, le droit à l'accès à l'information, alors même que cette circulation constitue le cœur de son activité. Que dire alors des cas où les moteurs de recherche suppriment l'accès à des contenus illicites qui leur sont signalés et qui peuvent aussi emporter un contrôle du respect des libertés d'expression, d'opinion ? Les moteurs de recherche ne pourraient exercer partiellement la fonction de régulation du droit au déréférencement qui leur a été assignée, bien malgré eux d'ailleurs.

Si l'on peut comprendre l'agacement de certains, cette critique est largement exagérée. Elle nous invite à rappeler ce qu'est un juge. Ce terme désigne une personne qui a le pouvoir de dire le droit, de trancher un litige. La mise en place du Comité Google pour l'aider à fixer sa propre doctrine[1] et le refus de Google d'implanter globalement le droit au déréférencement sont autant de manifestations de la volonté de cette entreprise d'influencer le droit. Il n'en demeure pas moins que Google ne tranche pas véritablement les litiges : il traite des demandes de déréférencement qui, ensuite, peuvent être soumises aux juges. Chaque décision prise par Google comporte d'ailleurs une information indiquant à la personne concernée qu'elle peut saisir le juge en cas de désaccord.

Presque quatre ans après l'arrêt Google Spain, il existe, à notre connaissance, une dizaine de saisines de juges français relatives à la mise en œuvre du droit au déréférencement.

Il est possible d'en déduire trois



Les saisines juridictionnelles françaises relatives au droit au déréférencement

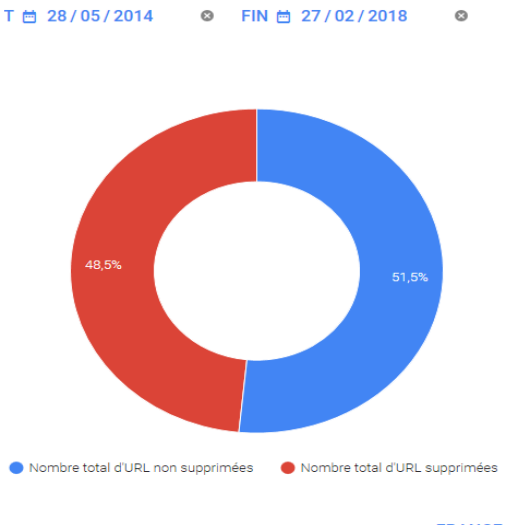
OliviaTambou

Cliquez sur le lien pour agrandir l'image https://blogdroiteuropeen.files.wordpress.com/2017/05/saisine-franc3a7aise-rtbf.png

enseignements. D'une part, le juge national est le juge de droit commun du droit au déréférencement. D'autre part, le juge national est le témoin de la nécessité de clarification du droit au déréférencement par la CJUE. Enfin, l'émergence du contentieux en matière de droit au déréférencement invite à s'interroger sur la montée en puissance du juge judiciaire dans le développement du droit à la protection des données personnelles.

I- LE JUGE NATIONAL : JUGE DE DROIT COMMUN DU DROIT AU DÉRÉFÉRENCEMENT

Avant 2014, les juridictions françaises étaient partagées sur la reconnaissance ou non d'un droit à l'oubli numérique[2]. Depuis elles ont pris acte de la décision de la CJUE et ont examiné en s'appuyant sur cette jurisprudence les recours qui leur ont été adressés.



Statistiques données par Google au 27 février 2018

La France est le pays européen dans lequel le plus grand nombre de demandes de déréférencement a été enregistré (497 697 au 5 mars 2018). C'est sans doute la raison pour laquelle, il est possible de constater d'emblée la diversité des types de saisines juridictionnelles. Afin de rendre compte de la spécificité de l'organisation juridictionnelle française, il est possible d'évoquer, d'une part, la saisine des juges judiciaires, d'autre part, les saisines du Conseil d'Etat.

A Le juge judiciaire français : arbitre des conflits de déréférencement entre entités privées

Une première série de litiges porte sur des refus de Google de déréférencer certaines URLs. D'autres affaires opposent des particuliers à des journaux. Dans les deux cas, s'agissant de litiges entre particuliers, ces affaires relèvent du juge judiciaire. Elles ont été traitées principalement par des Tribunaux de Grande Instance (TGI), et prennent la forme d'ordonnance de référé. Plus récemment la Cour de Cassation a eu l'occasion de rappeler l'obligation pour le juge d'examiner au cas par cas les suppressions d'URLs.

1°) Les TGI: Juges en référés des conflits de déréférencement entre particuliers

En droit français, les TGI traitent des litiges opposant des personnes privées (physiques ou morales) en fonction de la hauteur du montant du litige, ou de sa nature[3]. En outre, le président du TGI a une compétence de principe pour statuer en référé sur « toutes les mesures qui ne se heurtent à aucune contestation sérieuse ou que justifie l'existence d'un différend », selon l'article 808 du Code de Procédure Civile (ci-après CPC)[4] . Rappelons d'ailleurs à ce titre que, les ordonnances de référé relatives au déréférencement ont pour objet de faire cesser en urgence un trouble manifestement illicite au sens de l'article 809 du CPC.

Les juges ont fait usage de leur compétence de juge de référé afin de permettre à un justiciable d'obtenir la mise en œuvre d'une obligation découlant du droit de l'Union européenne, telle qu'interprétée par la CJUE dans son arrêt *Google Spain*. Chacune de ces ordonnances citent d'ailleurs explicitement l'arrêt *Google Spain*. De surcroît, chaque fois que le TGI a donné gain de cause à la victime, non seulement ses ordonnances adressent une injonction de déréférencement à la société Google Inc. et non à la société Google.fr mais certaines ordonnances

1. Voir notre tribune, Le rapport du Comité Google : exercice d'autorégulation d'un droit à l'oubli, Dalloz Actualité, Droits en Débats, 19 fev. 2015.
2. cf. pour l'affirmation de l'absence d'un droit à l'oubli, Cour d'Appel de Paris, 26 fév. 2014, http://www.village-justice.com/articles/Pas-loi-pas-droit-oubli,16474.html
3. N. Fricero, Tribunaux de Grande Instance (Organisation et compétence) Répertoire Dalloz, 2016, spécialement points 159 et s. 2. N. Fricero, Tribunaux de Grande Instance (Organisation et compétence) Répertoire Dalloz, 2016, spécialement points 159 et s.
4. Pour plus d'éléments sur le référé, voir : N. Cayrol, Le référé civil, répertoire Dalloz, 2016.
5. P TGI, Ord. de référé 16 sept.2014 M. et Mme X et M. Y / Google France https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-refere-du-16-septembre-2014/.

ont également assorti l'injonction d'astreintes afin d'accélérer leur exécution.

L'ordonnance de référé du TGI de Paris en date du 16 septembre 2014[5] est la première à faire expressément référence à l'arrêt *Google Spain*. Elle concerne néanmoins un cas de déréférencement de liens renvoyant à des contenus jugés diffamatoires par le Tribunal correctionnel de Paris. Dans cette espèce, le juge français a refusé de limiter son injonction à Google.fr en se fondant sur les propos tenus par la CJUE dans l'arrêt *Google Spain* sur l'unité entre Google Spain et Google Inc. en terme d'établissement. C'est d'ailleurs la raison pour laquelle ce n'est pas cette ordonnance, mais celle du 19 décembre 2014[6] qui est généralement considérée comme la première condamnation française à un déréférencement sur le seul fondement de l'arrêt *Google Spain*. Cette deuxième ordonnance trouve son origine dans un conflit qui opposait Google à la requérante, antérieurement au prononcé de l'arrêt *Google Spain*. La victime a décidé de saisir directement le juge pour obtenir la suppression de liens vers un article d'un journal relatant des faits d'escroquerie pour laquelle elle avait été condamnée huit ans auparavant. La publication reposait sur une information licite et la requérante n'avait pas cherché à obtenir son retrait directement auprès de l'éditeur du journal. Elle estimait que le maintien de ces liens par le moteur de recherche nuisait à sa recherche d'emploi. Le TGI a fait droit à sa demande en considérant que la requérante justifiait de raisons prépondérantes et légitimes prévalant sur le droit à l'information. L'ancienneté de la condamnation, le fait que celle-ci ne figure pas au casier judiciaire de la requérante ont été pris en compte dans cette appréciation. En outre, le TGI a adressé une injonction sous astreinte provisoire de 1000 € par jour de retard dans le délai de 10 jours à partir de la signification de l'ordonnance.
Dans une ordonnance du 13 mai 2016[7] , le TGI de Paris a par ailleurs considéré que le refus de Google de faire droit au déréférencement demandé par le requérant n'était pas justifié par le droit à l'information légitime du public. L'affaire est intéressante car elle illustre en quoi le déréférencement peut être une solution face à des personnes prétendant agir en tant que lanceur d'alerte, alors qu'en réalité leur but serait plutôt de nuire à la réputation d'une personne en répandant sur le web de fausses nouvelles, dont peu d'acteurs peuvent en réalité vérifier la véracité. En l'espèce, ni Google, ni l'hébergeur des URLs n'avaient accepté de retirer les contenus accusant le requérant d'avoir commis des actes de violences sexuelles sur une mineure. Le TGI s'est ici notamment appuyé sur le fait que l'article en cause, évoquait la profession de cette personne, nommant au passage son employeur, ce qui était dépourvu de lien avec les allégations dénoncées. Il a aussi constaté que la victime n'avait fait l'objet d'aucune condamnation en ce sens inscrite dans son casier judiciaire. Cette affaire illustre, en outre, parfaitement le parcours du combattant d'une victime d'une vindicte. Le requérant a dû utiliser toutes les voies possibles pour faire cesser cette injustice, y compris le signalement de contenus illicites auprès du gouvernement français et la saisine de la CNIL. Finalement, face au refus de Google de procéder au déréférencement, c'est devant le président du TGI de Paris que ladite victime a obtenu une injonction de déréférencement du lien litigieux, sans astreinte néanmoins, et une condamnation de Google à payer 2500€ à la victime au titre de l'article 700 du CPC. Le TGI donne cependant raison à Google sur certaines de demandes déréférencement dans la mesure où la victime n'a pas pu faire la preuve que le lien en cause apparaissait dans la liste des résultats générés en entrant son nom et prénom dans le moteur de recherche Google. Ce rejet atteste donc, non seulement de la difficulté que peut rencontrer une victime en matière de preuve, mais aussi sans doute des limites du droit au déréférencement, une information mise en ligne étant toujours susceptible d'être retrouvée d'une manière ou d'une autre et avec un peu perspicacité.

L'ordonnance de référé du TGI de Toulouse du 21 janvier 2015[8] constitue, quant à elle, l'une des rares décisions françaises dans laquelle, le juge reconnaît que Google a apporté la preuve de l'existence d'un intérêt

6. TGI Paris 19 décembre 2014: TGI de Paris (ord. réf.), 24 novembre et 19 décembre 2014 - Marie-France M. cl Google France et Google Inc. https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-de-refere-du-19-decembre-2014/.
7. TGI Paris, 13 mai 2016. Monsieur X. / Google France et Google Inc., https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-refere-du-13-mai-2016/.
8. Cette ordonnance n'a pas été publiée. Nous remercierons le greffe du TGI de Toulouse pour nous en avoir facilité la communication afin de faire cet article. Pour une analyse de cette ordonnance cf. Amélie Blocman, Droit à l'oubli : premières décisions rendues en application de la jurisprudence de la CJUE, Légigpresse http://merlin.obs.coe.int/iris/2015/4/article8.fr.html.

prépondérant du public à avoir accès aux informations litigieuses. Trois raisons principales ont été invoquées par le juge. La première raison est l'absence de renvoi « vers une information ayant trait à la vie privée du demandeur ». Les pages en cause relataient des informations sur sa vie professionnelle qui avait fait l'objet de décisions judiciaires rendues publiques et accessibles à tous. Elles évoquaient son licenciement pour harcèlement à l'égard de salariés. Le caractère récent des faits était la deuxième raison : ils dataient de 2011, soit de 4 ans. En outre, les faits ne pouvaient être qualifiés d'inexacts, d'inadéquats, de non pertinents ou d'excessifs, et ce d'autant plus que, le requérant n'avait pas entamé de procédure en diffamation. Enfin, le fait qu'une affaire judiciaire était en cours a constitué une raison supplémentaire pour faire prévaloir l'intérêt du public à être informé. Le TGI a alors condamné le requérant au versement d'une somme de 2000€ au titre de l'article 700 du CPC. De quoi sans doute inciter les requérants à s'interroger sur le bien-fondé de leur requête avant de saisir la justice.

La dernière ordonnance à mentionner est l'ordonnance du TGI de Paris du 10 février 2017[9]. Elle rappelle la nécessité de saisir préalablement Google d'une demande de déréférencement avant de demander un référé. Elle illustre, en outre, une nouvelle fois qu'une demande de déréférencement ne peut pas être prise en compte lorsqu'elle concerne une condamnation récente, en l'espèce moins de deux ans. Le référencement d'une information exacte sur un sujet d'actualité récent participe au droit à l'information du public. Il s'agissait, en l'espèce, d'une condamnation pénale d'un médecin pour des faits d'escroquerie à l'assurance maladie ayant conduit à une peine de quatre ans de prison et une interdiction définitive d'exercer la médecine.

2°) Les juges judiciaires : juge protecteur des organes de presse en ligne

La Cour de Cassation[10] a été amenée à trancher la question du statut des moteurs de recherche des organes de presse en ligne. Les requérants souhaitaient en réalité la suppression de leurs données à caractère personnel intégrées dans des archives en ligne d'un organe de presse. A l'appui de leur demande, ils arguaient que l'utilisation de leurs noms de famille comme mots clés sur le moteur de recherche de cet organe de presse faisait systématiquement ressortir un article relatant une condamnation ancienne.

Si l'objectif des requérants étaient d'inciter le juge à appliquer la jurisprudence *Google Spain* aux moteurs de recherche des organes de presse en ligne, les juridictions françaises ont globalement rejeté cette approche. Ces dernières ont considéré que la diffusion d'archives journalistiques en ligne bénéficiaient d'un régime dérogatoire fondé sur l'article 67§2 de la loi informatique et libertés. Autrement dit, le traitement en cause bénéficiait d'un intérêt légitime pouvant remettre en cause le droit d'opposition des requérants. La Cour de Cassation a considéré, comme la Cour d'Appel, que le retrait du nom et prénom des personnes visées dans les articles archivés, mais aussi la limitation de l'accès aux informations par une modification du référencement habituel « excède les restrictions qui peuvent être apportées à la liberté de la presse ». La Cour de Cassation a, en outre, à cette occasion rappelé que les journaux ne sont pas en principe tenus à l'anonymisation comme le sont les bases de données des décisions de justice. Il y a lieu de souligner que la loi 2004-81 a introduit en droit français un certain nombre de garanties relatives au traitement des données personnelles à des fins journalistiques. De tels traitements échappent à la limitation de la durée de conservation, à certaines interdictions relatives aux traitements de données sensibles notamment des données relatives aux infractions et condamnations. La possibilité pour les Etats membres de mettre en place des dérogations ou des exemptions particulières pour concilier protection des données personnelles et liberté d'expression, notamment la liberté de recevoir des informations, a été expressément prévue par la directive 95/46 et également à l'article 85 du Règlement Général de la Protection des données (RGPD). La loi française en appelle néanmoins à la responsabilité de la profession à faire usage de ces dérogations dans « le respect des

9. TGI Paris, ord. de référé: 10 février 2017: Monsieur X. / Google France et Google Inc. , https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-refere-du-10-fevrier-2017/.
10. Cour de Cassation, 1er civ. 12 mai 2016, n° 15-17.729 M. Stéphane et Pascal X.c/ Les Echos, https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000032532166 ; N. Metallinos Revue Communication-commerce électronique, juillet-août 2016.
11. TGI de Paris : 8 janvier 2016 F. B-H. / 20 Minutes France ; https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-refere-du-8-janvier-2016/.
12. E. Wery, Le droit à l'oubli peut-il aller jusqu'à entraîner la modification des archives de presse ?, https://www.droit-technologie.org/actualites/le-droit-a-loubli-peut-il-aller-jusqua-entrainer-la-modification-des-archives-de-presse/ ; E. Cruysman, Le droit à l'oubli divise les Cours de cassation française et belge, http://www.justice-en-ligne.be/article922.html.

règles déontologiques ».

Une solution similaire a été dégagée par le TGI de Paris dans une ordonnance de référé du 8 janvier 2016[11] .

En revanche, ces deux positions sont contraires à celle de la Cour de Cassation Belge rendue le 26 avril 2016[12] . La Cour de Cassation Belge a, sur le fondement de la responsabilité civile des éditeurs, jugé que « *le droit au respect de la vie privée (...) qui (...) comporte le droit à l'oubli permettant à une personne reconnue coupable d'un crime ou d'un délit de s'opposer dans certaines circonstances à ce que son passé judiciaire soit rappelé au public à l'occasion d'une nouvelle divulgation des faits, peut justifier une ingérence dans le droit de la liberté d'expression* ». Il est vrai que chacune des juridictions suprêmes étaient tenues par l'objet de leurs saisines et les particularités de leur droit national. L'existence dans le cas belge d'une décision de réhabilitation du requérant a donc été aussi un facteur déterminant dans la différence de solutions envisagées par les deux Cours. Il n'en demeure pas moins que des appréciations nationales différentes de l'exercice d'un droit au déréférencement pour les organes de presse est possible.

Il faut en déduire globalement qu'agir contre un site de presse plutôt que contre un moteur de recherche est plus aléatoire. La suppression des références à des données personnelles dans un article ancien de presse continue de se faire essentiellement en France sur la base d'une décision judiciaire constatant la diffamation, l'injure ou une atteinte à la vie privée.

3°) La nécessité d'un examen au cas par cas par le juge

Dans son arrêt du 14 février 2018[13], la Cour de Cassation a eu l'occasion de rappeler la nécessité pour les juges du fond d'examiner au cas par cas les demandes de désindexation d'URLs. Elle a rappelé que la CJUE exige que le juge vérifie l'existence d'un juste équilibre entre l'intérêt légitime du public pour l'information et les droits au respect de la vie privée et à la protection des données personnelles garanties par la Charte. En l'espèce la Cour d'Appel d'Aix en Provence avait ordonné la suppression de deux URLs précises à la Société Google. Elle s'était ensuite contentée d'adopter pour le reste une injonction générale de suppression d'URLs qui devaient être identifiées et signalées par le requerant lui-même comme portant atteinte à sa vie privée. La Cour de Cassation a considéré très justement que c'était à tort que la Cour d'Appel avait adopté une telle injonction d'ordre général. La Cour Suprême française rappelle ainsi l'importance du contrôle du juge qui doit trancher de manière précise le litige entre Google et un particulier pour chacune des URLs concernées.

B-Le Conseil d'Etat : traditionnel arbitre des recours contre les décisions de la CNIL

Une troisième série affaires sont pendantes devant le Conseil d'Etat. Elles ont été introduites contre des décisions de la CNIL. Rappelons, à ce titre, que les recours contre les décisions de la CNIL relèvent de l'ordre administratif et directement du Conseil d'Etat puisque cette dernière est une autorité administrative indépendante.

La première affaire a été à l'initiative de Google et concerne son différend avec la CNIL relatif au champ d'application géographique du droit au déréférencement. Les autres affaires connues ont été introduites par des particuliers en désaccord avec la décision de la CNIL qui a soutenu la position de Google pour le non-déréférencement d'URLs qu'ils avaient demandés. Il s'agit de quatre affaires portant sur des demandes concernant principalement le traitement de données dites sensibles au sens de l'article 8 de la directive 95/46 et lesquelles ont fait l'objet par le Conseil d'Etat d'un renvoi préjudiciel devant la CJUE le 27 février 2017 [14] .

II- LE JUGE NATIONAL : TÉMOIN DE LA NÉCESSITÉ DE CLARIFICATION DU DROIT AU DÉRÉFÉRENCEMENT PAR LA CJUE

Le Conseil d'Etat est à l'origine d'une série de questions préjudicielles relatives à la mise en oeuvre du droit au déréférencement. Ces interrogations sont relatives au traitement de données sensibles et des condamnations pénales d'une part, et à l'ampleur du champ géographique d'autre part.

A-La spécificité des traitements de données sensibles

Le Conseil d'Etat a introduit, le 27 février 2017, un

13. Cour de Cassation, 1ère Chambre civ., arrêt n°178, du 14 février 2018, *Société Google c. Thierry X.*, ECLI:FR:CCASS:2018:C100178, https://www.courdecassation.fr/jurisprudence_2/premiere_chambre_civile_568/178_14_38605.html
14. CE 24 février, Mme C, M.F, M.H, M.D, n° 391000, 392768, 399999,401258, https://www.legifrance.gouv.fr/affichJuriAdmin.do?&idTexte=CETATEXT000034081835.

ensemble dense de quatre questions préjudicielles devant la CJUE.

Premièrement, le Conseil d'Etat souhaite savoir dans quelle mesure l'interdiction de traitement de données sensibles et de données relatives aux infractions, condamnations pénales ou aux mesures de sûretés s'applique aux moteurs de recherche en tant que responsable de traitement.

Deuxièmement, le Conseil d'Etat pose une série de questions dans l'hypothèse où la CJUE reconnaîtrait que ces interdictions de traitement s'appliquent aux moteurs de recherche. Le Conseil d'Etat interroge la CJUE quant à l'existence dans ce cas d'une obligation pour le moteur de recherche de faire droit aux demandes de déréférencement de telles données. Le Conseil d'Etat demande à la CJUE de préciser si le moteur de recherche peut refuser le déréférencement en se fondant sur certaines exceptions relatives au traitement des données sensibles[15]. Il s'agit, d'une part, du cas où la personne a donné son consentement explicite et, d'autre part, des cas où « le traitement porte sur des données manifestement rendues publiques par la personne concernée ou est nécessaire à la constatation, l'exercice ou la défense d'un droit en justice »[16]. Le Conseil d'Etat interroge aussi la CJUE quant à la possibilité pour un moteur de recherche de se prévaloir de la dérogation applicable aux traitements de données personnelles effectuées aux seules fins de journalisme dans certains cas. Il s'agit de l'hypothèse où les liens dont le déréférencement est demandé concernent des articles de presse entrant dans cette dérogation.

Troisièmement, en l'absence d'application des interdictions de traitement des données sensibles par le moteur de recherche, la CJUE est appelée à clarifier les exigences spécifiques que l'exploitant d'un moteur de recherche doit remplir. Le Conseil d'Etat souhaite en particulier que la CJUE se prononce sur la portée des obligations du moteur de recherche lorsque les pages vers lesquelles renvoient les liens, comportent un traitement illicite de données personnelles. Doit-il supprimer de droit ces liens ou prendre en compte la circonstance de cette illicéité pour apprécier le bien-fondé du déréférencement ? Le Conseil d'Etat demande, en outre, si les obligations du moteur de recherche peuvent être différentes lorsque la cause de l'illicéité du traitement des données personnelles sur la page d'origine relève en fait du droit national et non du droit de l'Union européenne.

Enfin, la quatrième question porte sur la marge de manœuvre des moteurs de recherche lorsqu'il est établi que la publication, vers laquelle les liens renvoient, repose sur des données personnelles qui sont incomplètes, ou inexactes. Le moteur de recherche a-t-il dans de telles hypothèses l'obligation de faire droit à la demande ?

Finalement, le Conseil demande si les informations relatives à la mise en examen d'un individu ou relatant un procès qui en découle doivent être interprétées comme des données relatives aux infractions et aux condamnations pénales au sens de l'article 8 §5 de la directive 95/46.

Dans un discours sur la liberté d'expression à l'âge d'Internet, le Vice-Président du Conseil d'Etat a résumé l'enjeu des questions posées par sa juridiction : « … *cette jurisprudence doit-elle se traduire par l'interdiction de tout traitement des données sensibles, telles que définies à l'article 8 de la directive de 1995, ou doit-elle conduire à articuler ces dispositions avec la liberté d'expression, à laquelle concourent les moteurs de recherche, en encadrant strictement les obligations de déréférencement* ? »[17] .

Par ailleurs, comme dans les affaires judiciaires précédentes le Conseil d'Etat rappelle que le traitement des données personnelles opéré par le moteur de recherche exploité par Google Inc. entre dans le champ d'application de la loi française sur la protection des données personnelles. Il se fonde sur le droit d'opposition[18] inscrit à l'article 38 de la Loi informatique et Libertés considérant que cette disposition assure la transposition des articles 14a) et 12b) de la directive 95/46 et sur l'arrêt *Google Spain* pour constater l'existence d'un droit au déréférencement. Il rappelle ensuite la compétence de la CNIL pour examiner les demandes de déréférencement et sa compétence en tant que juge pour excès de pouvoir pour examiner les décisions prises par la CNIL à cet égard.

15. Article 8§1 de la directive 95/46.
16. Article 8§2 de la directive 95/46.
17. Introduction de Jean-Marc Sauvé lors de la conférence sur la « liberté d'expression en ligne » organisée par la Présidence chypriote du Conseil de l'Europe à Nicosie, à l'invitation de la Cour Suprême de la République de Chypre le 28 avril 2017 http://www.conseil-etat.fr/Actualites/Discours-Interventions/La-liberte-d-expression-a-l-age-d-Internet
18. Cela illustre encore une fois l'ambiguïté de la nature du droit consacré dans l'arrêt Google Spain évoquée dans notre article précédent : cf. nos propos introductifs p. 23 et s.

B-Le champ d'application géographique du droit au déréférencement

Cette question oppose la CNIL à Google. La CNIL considère qu'il existe une unité du traitement des données à caractère personnel par Google à l'échelle mondiale qui justifie que seul un déréférencement à l'échelle mondiale est acceptable. Google de son côté estime que le droit au déréférencement est un droit européen et ne s'applique que sur le territoire de l'Union européenne. Il refuse un déréférencement mondial qui le placerait inévitablement en violation dans certains États au regard de la liberté d'expression ou du droit à l'information. Il propose que le déréférencement ne soit mis en œuvre que lorsque la recherche s'effectue en Europe. Selon la CNIL, cette solution n'a pas de sens. Sa présidente considère que «Le droit au déréférencement n'est pas un droit "à ne pas voir" localement que Google traite vos données ; c'est un droit à ce que Google ne traite pas certaines de vos données. Retenir l'hypothèse inverse reviendrait à vider les droits des Européens de leur substance et à considérer que la portée d'un droit fondamental est à géométrie variable, dépendant non de celui qui l'exerce, mais de celui qui en regarde les résultats.»[19] L'argument est intéressant, car il repose sur la fondamentalisation du droit à la protection des données personnelles. Cela dit, il rend le conflit inextricable. Face à cette difficulté sérieuse d'interprétation, le Conseil d'État a récemment saisi la CJUE afin qu'elle détermine clairement quelle est l'ampleur géographique du droit au déréférencement[20]. Il s'agit de choisir entre les deux options actuellement débattues entre la CNIL et Google. La solution prônée par la CNIL est celle d'un déréférencement mondial. La solution mise en œuvre par Google, est celle d'un déréférencement européen incluant des mesures dites de « géoblocage» visant à rendre la consultation des extensions non européennes impossibles pour les requêtes faites à partir d'une adresse IP localisée dans un État membre de l'Union européenne. Le Conseil d'État interroge également la CJUE sur la pertinence d'une troisième option qui était celle envisagée au départ par Google. Il s'agit de la possibilité d'un simple déréférencement national, c'est-à-dire dans l'extension nationale de l'État membre dans lequel la demande de déréférencement a été effectuée[21]. Autrement dit, le déréférencement se ferait uniquement sur google.fr pour un français ou un résident français.

L'ultime leçon à tirer de ces développements est, peut-être, l'émergence d'un contentieux en droit de la protection des données personnelles dans lequel le juge, et en particulier en France, le juge judiciaire français, pourrait devenir un acteur incontournable.

III- LE JUGE JUDICIAIRE FRANÇAIS, FUTUR ACTEUR INCONTOURNABLE DU DROIT DE LA PROTECTION DES DONNÉES?

L'intérêt d'une plus grande implication du juge dans le développement du droit de la protection des données est évoqué depuis longtemps[22] . Cette revendication dépasse largement le cadre de l'Europe ; elle est d'ailleurs actuellement débattue outre-Atlantique[23] .

En France, cette question peut s'analyser comme une nouvelle illustration du dialogue compétitif des juges dans la protection des libertés et des droits fondamentaux. L'ordre administratif, et en particulier le Conseil d'Etat, a pu être considéré comme le juge de droit commun en matière de protection des données personnelles. Aujourd'hui, certains auteurs[24] , des discours[25] réaffirment la nécessité, l'intérêt d'une montée en puissance du juge judiciaire, étant donné le rôle de garant des libertés individuelles que lui accorde la Constitution. Les juges judiciaires pourraient s'imposer dans la mise en œuvre du droit au déréférencement. L'intérêt des particuliers dans l'utilisation du référé civil afin d'obtenir gain de cause contre les refus de déréférencement des moteurs de recherche en est l'illustration.

L'introduction en France d'une action de groupe[26] en matière de protection des données personnelles pourrait également avoir pour effet d'augmenter les saisines judiciaires visant à faire cesser des violations de la loi française informatique et libertés par des responsables de traitement. Les litiges opposant les associations représentantes du groupe aux opérateurs privés responsables de traitement relèvent des juridictions civiles. Il est fort peu probable néanmoins que cela puisse s'appliquer aux demandes de déréférencement qui nécessitent un examen au cas par cas. En effet,

19. Tribune d'Isabelle Falque-Perrotin publiée dans Le Monde du 29 décembre 2016
20. Cf. CE, 19 juillet 2017, n°399922, RFDA 2017 p. 1479 avec les conclusions de Mme Aurélie Bretonneau cf. annexes
21. Selon le rapporteur public un tel déréférencement national a été mis en œuvre par une Cour régionale de Hambourg.
22.Lee A. Bygrave, "Where have all the judges gone? Reflections on judicial involvement in developing data protection law", Privacy Law & Policy Reporter, 2000, volume 7, pp. 11–14, pp. 33–36] accessible http://folk.uio.no/lee/oldpage/articles/Judges_role.pdf.
23. B. Boliek, "Prioritizing Privacy in the Courts and Beyond (March 05, 2017)", Cornell Law Review, Vol. 103 (Forthcoming). Available at SSRN: https://ssrn.com/abstract=2959636.
24. C. Bloud-Rey, « Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles? Analyses et perspectives », Dalloz, 2013, p. 2795.

cette action collective exige que les personnes physiques formant le groupe soient « placées dans une situation similaire (et) subissent un dommage ayant pour cause commune un manquement de même nature aux dispositions » de la loi française relative à la protection des données personnelles. La montée en puissance du juge judiciaire français pourrait être liée aux modifications introduites par le RGPD, mais ceci fera l'objet d'une contribution ultérieure.

En guise de conclusion, on peut s'interroger sur le caractère pérenne du développement du contentieux juridictionnel du droit du déréférencement. Une fois le régime de ce droit mieux clarifié par les juges, la marge de manœuvre des moteurs de recherche précisée, la régulation pourrait continuer de s'affirmer comme la voie privilégiée pour assurer la mise en œuvre de ce nouveau droit. En attendant, l'existence de peu de saisines juridictionnelles atteste encore une fois de la nécessité de plus de transparence dans la régulation du droit au déréférencement par les moteurs de recherches et la CNIL[27].

25. Cf. B. Louvel, Premier président de la Cour de Cassation : L'autorité judiciaire : gardienne de la liberté individuelle ou des libertés individuelles ? du 2 février 2016 https://www.courdecassation.fr/publications_26/discours_entretiens_2039/discours_2202/premier_president_7084/gardienne_liberte_33544.html.
26. Loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle, article 91.
27. id. cf. nos propos introductifs p.27

THE 'RIGHT TO BE FORGOTTEN' AS THE RIGHT TO REMOVE INCONVENIENT JOURNALISM? AN ITALIAN PERSPECTIVE ON BALANCING THE RIGHT TO BE FORGOTTEN WITH THE FREEDOM OF EXPRESSION

By Giulia Tiberi
Adjunct Professor of Constitutional Law, University of Insubria, Varese-Como, Italy

The essay, while acknowledging the "multiple" meanings that the "right to be forgotten" displays in the Italian legal system after the Internet revolution, analyses – in the aftermath of the CJEU's landmark decision in 2014 in *Google Spain* – how national courts and the Italian Data Protection Authority have thus far tried to find a fine tuned equilibrium between the right to be forgotten and freedom of expression, mostly confirming and even reinforcing that no right to be forgotten can be claimed for data in the public interest. Still, a recent decision of the Italian Supreme Court appears to be going against the tide, reaching conclusions that could result in unprecedented constraints on news media, clearly disregarding the principles settled at supranational level both by the CJEU and by the ECtHR.

Keywords: right to privacy; right to be forgotten; freedom of expression; data collection; access to information.

The digital era has dramatically broadened and deepened the existential contradiction human beings experience in their lives,[1] as

> "On the one hand, they aspire to immortality, and, knowing that they cannot have it, they try to leave the memory of themselves for as long as possible as the only way to prolong their life, or rather their memory into the future that they existed, and what they achieved. (...) Conversely, every person also has the terror that every negative act committed in the course of their existence can be remembered forever or at least while he is alive and so are the ones who have memory"[2].

Intense legal, but also philosophical[3], debates in recent years have tackled issues of paramount importance in contemporary society, such as the role of oblivion in social interaction[4], the increasing amount of data and information available on the internet that shapes individual identity, and the ever growing role of private entities in gathering information for and about users. These debates have clarified that under the label of "oblivion" and "forget", there are two dimensions to be considered at the same time, the "right to forget" and the "right to be forgotten"; not two different rights, but two different features of the same right encompassing two different concepts[5]. While the "right to forget" can be framed as the right not to be accountable for one's conduct after a certain amount of time and beyond a given framework of relationships, the "right to be forgotten" encompasses the right not to see one's past coming back forever (the older the origin of the information goes back, the more likely personal interests will prevail over public interests).

These concepts, in particular the latter one, raise

1 The article is part of a research run as academic coordinator of the Jean Monnet Module "Personal data protection as a fundamental right in the EU in the digital age - A dialogue among constitutional law, criminal law, civil procedure law and judicial protection of IP rights". The author wishes to thank the anonymous reviewers for their comments.
2 According to former President of the Italian Data Protection Authority and constitutional scholar Franco Pizzetti, 'Privacy e il diritto europeo alla protezione dei dati personali: dalla direttiva 95/46 al nuovo regolamento europeo,' (2016, Giappichelli Editore) p. 20 (translated from Italian).
3 Ugo Pagallo and Massimo Durante, 'Legal Memories and the Right to Be Forgotten' (2014) in L. Floridi (ed.), Protection of Information and the Right to Privacy – A New Equilibrium?, Springer , pp. 17-26.
4 Viktor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, (2009).
5 Gregory W. Streich, 'Is There a Right to Forget? Historical Injustices, Race, Memory, and Identity', (2002) New Political Science, Vol. 24/4, pp. 525-542; Rolf H. Weber, 'The Right to Be Forgotten: More Than a Pandora's Box?', 2 (2011) JIPITEC 120; Franco Pizzetti, 'Is there a fundamental right to forget?', Intervention at the Conference organised by the European Commission "Personal data: more use, more protection", Brussels 19 May 2009.

several sensitive questions, as it is highly questionable until when, to what extent, and by whom should our past be known. For instance, should a person be accountable for past conduct, or even should past conduct be made known to entities other than those entitled to know because of the specific tasks discharged and/or because of their relationships with the data subject?[6] Striking a correct balance between privacy and freedom of expression has become an enigma, which is increasingly problematic to solve in the digital environment, because balancing those competing rights and interests reflects values weighed and perceived differently at the global level. This is clearly shown by the contrast between the American approach, considering preeminent the freedom of expression over the right to privacy, and the European approach where privacy is to trump freedom of speech[7]. In the "age of the algorithm" and the a-territorial dimension of the Internet, we are running into ever growing difficulties in defining the responsibilities of online service providers.

Considering the multitude of terms that have been used in recent years in the legal literature, (right to forget, right to erasure, right to delete, right to oblivion, right to social forgetfulness),[8] the prevailing "right to be forgotten" is, despite its catchy terminology, quite a generic expression that often does not do justice to the concepts it means to convey. Indeed, it can be misleading if it is not grounded in a specific legal tradition and investigated through the looking glass of its judicial enforcement.

This is the preliminary reason of interest for a deeper understanding of a "right to be forgotten" from the Italian perspective, bearing in mind that this right arose well before the emergence of the Internet and was developed before and independently from the adoption of the national legislation on personal data protection, which entered into force in Italy by the end of 1996 and continues to remain distinct from the right to data protection, as based upon different conditions[9].

This essay will thus consider, in the first instance, how the "right to be forgotten" is recognised and protected in Italy, so to clarify that the expression is nowadays used to reflect three different meanings[10], with the adjustment to its original understanding of two new dimensions that have been heavily influenced by the Internet revolution.

Special attention will then be devoted to considering, in the aftermath of the "copernican revolution"[11] brought about by the CJEU's landmark decision in 2014 in *Google Spain*[12] - a truly "Pandora's Box" ruling according to some Italian scholars[13] - how national courts and the Italian Data Protection Authority have thus far tried to find a fine tuned equilibrium between the right to be forgotten and freedom of expression, mostly confirming and even reinforcing that no right to be forgotten can be claimed for data in the public interest.

Still, a recent decision of the Italian Supreme Court appears to be going against the tide, reaching conclusions that could result in unprecedented constraints on news media. In departing from the guiding principles assessed at the supranational level, clearly misperceived by the Italian court, the question this ruling raises is quite a weird one: can the right to inform have an "expiry date"?[14]

Such issues obviously reveal the ongoing need for

6 Franco Pizzetti, 'Is there a fundamental right to forget?', nt. 3. See also Oreste Pollicino and Marco Bassini, 'Reconciling Right to be Forgotten and Freedom of Information in the Digital Age: Past and Future of Personal Data Protection in the European Union', (2014) Diritto pubblico comparato ed europeo, 641.

7 Mariarosaria Taddeo and Luciano Floridi, 'The Debate on the Moral Responsibility of Online Service Providers' (2016) Sci. Eng. Ethics, vol. 22, issue 6, 1575-1603.

8 See, among others, Cécile de Terwangne, 'Internet Privacy and the Right to Be Forgotten/Right to Oblivion' (2012) 13 IDP Revista de Internet, Derecho y Política 109, 115; Napoleon Xanthoulis, 'Conceptualising a right to oblivion in the digital world: A human-rights based approach', (2012) UCL research essay 16; Aurelia Tamo, Damian George, 'Oblivion, Erasure and Forgetting in the Digital Age', (2014) JIPITEC 71; Paul Bernal, 'A Right to Delete?' (2011) European Journal of Law and Technology 1.

9 Maria Angela Biasiotti, Sebastiano Faro, 'The Italian perspective of the right to oblivion' (2016) International Review of Law, Computers & Technology, 30:1-2, 5-16.

10 See Giusella Finocchiaro, 'Il diritto all'oblio nel quadro dei diritti della personalità' (2015) in 'Il diritto all'oblio su internet dopo la sentenza Google Spain', (2015 Roma TrE-Press), pp. 29 - 42; Maria Angela Biasiotti & Sebastiano Faro, cit..

11 See the Italian DPA Secretery General Giuseppe Busia, 'Una vera rivoluzione copernicana', (2014) Il Sole 24 Ore, 14 May 2014, p. 25.

12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* C-131/12 (ECJ, May 13, 2014),

13 Franco Pizzetti, 'La decisione della Corte di Giustizia sul caso Google-Spain: più problemi che soluzioni', (2014) Federalismi.it , 10 June 2014, 5; Tommaso Edoardo Frosini, 'Google e il diritto all'oblio preso sul serio', (2014) Il diritto dell'informazione e dell'informatica, 563.

14 For a first comment Guido Scorza, 'A ruling by the Italian Supreme Court: news do "expire". Online archive would ned to be deleted", (2016) L'Espresso, 1 July.

a deeper reflection on how to reconcile, within the "Web's memory" era, the right to be forgotten with the freedom of the press so as to prevent the "tyranny of values" of an absolute protection of the individual dimension, undermining the right to seek, receive and impart information of public interest, as a basic condition for democracy and political participation, together with the creation of a collective memory.

I-THE KALEIDOSCOPE OF THE "RIGHT TO BE FORGOTTEN" IN THE ITALIAN LEGAL SYSTEM.

A-The traditional concept

The concept of the right to be forgotten is not new from the perspective of Italian case law and scholarship.

The traditional concept of the "right to be forgotten" in the "offline environment" was conceived as a derivation of the protection of personal identity, as a specific safeguard arising in the context of the right to information,[15] to be granted when balancing the person's rights with the conflicting freedom of information guaranteed by Article 21 of the Constitution. In a nutshell, the right to be forgotten has originally been construed as the individual's right to avoid being perpetually stigmatised as a consequence of past actions, thus as the right of any individual to see himself represented in a way that is not inconsistent with his current personal and social identity. The aim is clearly not to prevent the publication of information, but an unjustified new publication of a piece of information, which had already been lawfully disseminated in the past but at a certain moment lacking a public interest to further circulate it.

Although in the Italian legal order no specifc legal provision foresees the right to be forgotten, since the mid-1990s courts and, later on also the Italian Data Protection Authority, recognised and protected the 'diritto all'oblio' – a term borrowed and inspired by the corresponding French expression 'droit a` l'oubli'- immediately deriving it from the provision set forth in Article 2 of the Italian Constitution[16] interpreted as a clause recognising "new fundamental rights" which are not expressly included in the Constitution.

Within this initial perspective, the term 'right to be forgotten' refers to the individual's right to protect their own private sphere from the publication and dissemination of facts or news when there is no public interest for the news story to 'lawfully circulate again, notwithstanding having being lawfully disseminated in the past'.

In the traditional "offline environment", the passage of time makes the public interest to know about a news story progressively fade and ultimately disappear. This explains the paramount importance vested by the time factor within the original meaning of the right to be forgotten, as time lapse becomes a crucial parameter to taken into consideration for evaluating a lawful treatment of personal data[17].

The test used by the Italian courts, for balancing the conflicting rights to privacy and personal identity with freedom of information, is based on the following parameters: a) the time elapsed since the first publication and the existence of the public interest in the information, namely the social value of the news; b) the modalities utilised for the publication of individual's information, namely the truth of the information to be re-published and the formal fairness of the exposition respectful of the person's dignity; c) the person's role in the fact, whether a public figure or not.

As made clear in a decision of the Italian Supreme Court (Corte di cassazione[18]) in the late 1990s

> "it is not lawful to disseminate again, after a substantial time, a news story that had been lawfully published in the past except when the facts previously published, due to other events that have occurred, again become current and a new interest in accessing such information arises even if not closely related to the simultaneity of the disclosure and the event."[19]

In such cases, when the right to be forgotten is recognised as prevailing over freedom of information of the press, the individual is granted a right to obtain from the courts the prohibition or the inhibition of the renewed dissemination of the information and the compensation for the damages suffered by the individual.

15 See Biasiotti-Faro, cit., p. 6; Franco Pizzetti,'Il prisma del diritto all'oblio' (2013) in Il caso del diritto all'oblio (ed. F. Pizzetti, Giappichelli), 21-63.
16 Article 2 of the Italian Constitution states: 'The Republic recognizes and guarantees the inviolable rights of the person, both as individual and in the social groups where human personality is expressed'.
17 As Biasiotti and Faro discuss, cit. nt. 6, 'because the right to such protection arises when time has passed and, due to this elapsing, the dissemination of personal information might be of no more interest for the general public', 7.
18 For further information on the Italian judicial system, see https://ejustice.europa.eu/content_judicial_systems_in_member_states-16-it-en.do?member=1 (accessed 12 April 2017)
19 Italian Supreme Court decision no. 3679/1998.

B-The new dimensions in the digital environment: the online archives and the "right not to be found/ seen"....

The advent and the development of new technologies and the Internet, with the drastic shift caused from a "default of forgetting" to a "default of remembering"[20], inevitably changed such scenario.

The "Web's memory"[21] (making indefinitely accessible for an unlimited number of persons information and personal data published online), boosted by the concurrent action performed both by search engines (allowing any user to retrieve published information, even past or parts of those, regardless of the actual location, and to aggregate those, often without contextualising them), and by big data processing techniques (capable of extracting not only explicit knowledge, but also the implicit) made evident the need for new protection measures against a misleading picture of the individuals, which may be sketched by past aspects that have never disappeared, no longer consistent with the current personal identity, becoming potentially harmful[22].

As it has been precisely argued,

> the time factor, so important in the original perception of the right to be forgotten, assumes a new meaning: the issue at stake now is that the publication of news is permanent and therefore the factor compressing the individual's personal rights is not the renewal of the publication but the permanent duration of it together with its stable circulation.[23]

All this has become evident in Italy with the migration of newspaper archives onto the Web: online journalism and the rapidly expanding sector of historical archives of digital publications, accessible free of charge and, even sometimes, over a time span of decades, raised new challenges with the enlargement of the conflicting rights and interests at stake that need to be balanced. News characterized by its persistence on the web and its connected easy availability through search engines, also going a long way back in time, may contain information about individuals that is very delicate, and almost always negative. This news, even if initially justified by proper exercise of the freedom of the press, then surely legitimised in their conservation by historical memory, needs enduring study and research, 'not infrequently reverberate (for an indefinite time) a negative and often conditioning influence on life and on the future expectations of many people'[24].

Thus, in the approach developed by the Italian Data Protection Authority in two leading cases in 2005 and 2008 concerning online archives,[25] the right to be forgotten in the digital environment has been reframed as a "right not to be found"[26] or as a "right not to be seen"[27] (a concept also lying at the bottom of the CJEU's judgement in *Google Spain*), considering that in the digital environment the term "right to be forgotten" is misleading and actually, as it has been thoroughly argued,[28] is quite impossible from a technical point of view, to be enforced on the Web.

On the contrary, such a "right not to be found", according to the Italian DPA, is to be pursued by controlling and limiting the indexability of personal data by general search engines external to the newspaper websites, but leaving the news accessible from inside the newspaper website and archive by means of the specific search function.

In balancing the individual right with the freedom of expression, the freedom to exercise free historical research, the right to education and information, as well as the rules on protection of personal data, the Italian DPA held that there were legitimate grounds for publishing the contested publication, as the facts were still of public interest, and the personal data stored

20 Viktor Mayer-Schonberger, 'Delete: The Virtue of Forgetting in the Digital Age' (Princeton University 2009) 25-28
21 See from an Italian perspective, Giusella Finocchiaro 'La memoria della rete e il diritto all'oblio' in Dir. Inf. 2010, p. 391 ss. Stefano Rodotà, Il diritto di avere diritti, (2012 Laterza).
22 Cecile de Terwangne, nt. 6, 115.
23 Biasiotti-Faro, cit., p. 8. See accordingly Giusella Finocchiaro, nt. 4.
24 Italian Data Protection Authority, 2013 Annual Report, p. 135.
25 Italian Data Protection Authority, Decision Oblivion Rights, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1336892; Decision December 11, 2008, 'Archivi storici on line dei quotidiani: accoglimento dell'opposizione dell'interessato alla reperibilità delle proprie generalità attraverso i motori di ricerca', doc. web no. 1583162, online: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1583162; See also Decision 8 April 2009, doc. web no. 1617673 and Decision 25 June 2009, doc. web no. 1635966.
26 See Franco Pizzetti ed. 'Internet e la tutela della persona. Il caso del motore di ricerca' (2015 Passigli Editori) and especially the essays of Lorella Bianchi and Giuseppe D'Acquisto, 'Il trattamento dei dati personali effettuato dai motori di ricerca, le esternalità prodotte sugli interessati e il diritto di rettifica. Quali prospettive e limiti dopo la sentenza della Corte di giustizia; Manuela Siano and Laura Tempestini, 'Il diritto di rettifica e di cancellazione dati. Il Regolamento europeo e gli interventi più significativi del Garante'.
27 Manuela Siano, 'Il diritto all'oblio in Europa e il recente caso spagnolo, in F. Pizzetti, Il caso del diritto all'oblio, (2013 Giappichelli) 132.
28 Giuseppe D'Acquisto, 'Diritto all'oblio: tra tecnologia e diritti',(2013) in 'Il caso del diritto all'oblio' (Franco Pizzetti ed. Giapplichelli), 103.

THE RIGHT TO BE FORGOTTEN IN ITALY

could not be deleted being part of an online newspaper archive that had to be safeguarded for historical research and news story aims.

On the other side, the DPA argued that there were no legitimate grounds for personal data in online archives being retrievable through external search engines, thus requiring any archive's web page containing personal data and news on the plaintiff's personal sphere and identity to be de-linked from the external search engine function by the data provider (at that time the company acting as the content provider, i.e. the newspaper publisher). With this solution – making news in their integral version only accessible from inside the online archive using the specific searching tool – the Italian DPA have struck a reasonable balance among several concurring, but conflicting, values, such as the preservation of the historical memory, the freedom of historical research and information, and the protection of the personal sphere[29].

C-....Online archives and the "right to a contextualised/updated information" and "the right to data deletion"

Still, the legal thinking on the right to be forgotten in the digital era has brought about a third new dimension of this right, according to the landmark decision adopted by the Italian Supreme Court in 2012[30], arising from a different perspective from the one initially discussed by the Italian DPA seen above.

It is interesting to observe that with this ruling the Italian Supreme Court overturned previous decisions on the same case held by both the Italian DPA and a lower court.

The case arose from a lawsuit launched by an Italian politician who, in 1993, had been arrested and charged with corruption, but later acquitted. Years later, having discovered that the only article retrievable online in the search engine results made reference exclusively to his arrest without any further clarification as to the positive development and solution of the case, he requested first from the Data Protection Authority and then the Regional Court of Milan the removal of the judicial data referring to him, claiming the violation of his rights under the Italian Data Protection Code,[31] complaining about the incomplete and non-updated online news regarding him. This led him to ask that the news article regarding his arrest be removed from the online archive of the newspaper "Corriere della Sera", which was still indexed by search engines or, in alternative, the insertion by the newspaper publisher of an updated link to the subsequent positive news, or the transfer of the news item to a section of the newspaper website, which was not indexed by external general search engines.

In the first instance the Italian DPA, as well as a lower civil court, in rejecting these requests, held that the online publication was lawful provided that the treatment of personal data without the consent of the subject were the exercise of the freedom of expression in the press.

On the contrary, the Supreme Court came to a different conclusion. Actually, the Court did not accept the claimant's ground for libel, as it recognised that the article had reported true facts at the time of its publication, but in any case the Supreme Court acknowledged that it had to grant a protection to the individual in the digital era to preserve his real and true identity, thus conceiving a new dimension of the "right to be forgotten" as "the right to a contextualised and updated information" or even – but only as long as "there is no public interest in knowledge of the news" – a "right to data deletion".

If then, for the individual, a right to updating the news has to be granted, otherwise - quoting the Supreme Court – "news become biased and inaccurate and therefore untrue" (emphasis added), which led some scholars to discuss "a right to the truth at the present time",[32] a corresponding obligation has been imposed on online newspapers, which is quite problematic; namely, an obligation to update their online archives through equipping them with "an appropriate system designed to provide information (in the body of text or in the margin) on whether there exists a follow-up or any development to news items and if so what the content is (...) allowing users swift and easy access to the updated information".[33]

Thus, in deciding the specific case, the Supreme Court held that, the right to privacy is limited by the freedom

29 Italian DPA, Decisions: 9 November 2005, no. 1200127; 11 December 2008, no. 1583162 and 1582866; 15 January 2009, no. 1589209; 18 March 2010, no. 1712827; 16 June 2010, no. 1734973; 21 March 2012, n. 1892254. See Alessandro Mantelero, 'Il diritto all'oblio dalla carta stampata a Internet', (2013) Il caso del diritto all'oblio (Franco Pizzetti ed. Giappichelli) 163.

30 Italian Supreme Court, Third Civil Division, judgement no. 5525 of 2012.

31 Legislative Decree no. 196 of 2003, 'Italian Data Protection Code'.

32 Giusella Finocchiaro, 'Italian Supreme Court affirms the right to information contextualization and to the current truth', in www.blogstudiolegalefinocchiaro.com (last accessed 30 April 2017).

33 Italian Supreme Court, Third Civil Division, judgement no. 5525 of 2012.

of expression only to the extent that there is a public interest in the news (as precisely happened in the case, where the political figure of the claimant perpetrated the general relevance of his arrest), due to the fact that if the news reported was to be considered incomplete in the light of subsequent events, a violation of the right to a coherent and updated identity of the person had to be recognized according to the provisions set forth in Articles 10 and 7 of the Italian Data Protection Code,[34] requiring personal data to be accurate and, where necessary, kept up to date. Therefore, entitling the data subject to ask for their updating, rectification, integration, or otherwise their erasure, anonymization or blocking if processed unlawfully, including data whose retention is unnecessary for the purposes for which they have been collected or subsequently processed.

It is quite interesting also to observe that the Supreme Court, even if almost in passing, held that the search engine service provider had no role or responsibility in the matter, thus rejecting one of the arguments of the defendant, who had claimed his lack of locus standi in favour of Google. The Italian Court thus was anticipating the same conclusion the Advocate General would have supported one year later in the *Google Spain* case, a conclusion that, as we know, the Court of Justice completely overturned in its decision.

Now, the 2012 Italian Supreme Court decision on online archives has received opposing comments in the Italian legal literature. A few scholars have highlighted its innovative approach, in taking into consideration both an individual and collective perspective, as the Supreme Court tried to safeguard at the same time, not only the right of the persons involved in the events to protect their own personal and moral identity, but also, the right of users of online newspapers to receive accurate and complete information.[35] Still, the majority of comments have heavily criticised it, not only for the huge economic duty de facto imposed on online newspaper archive providers – required to set up a constant updating system of all items published online –, but also for its "potentially explosive" conclusions from a legal standpoint in case of failure to comply with the said obligation; being exposed not only to civil actions for damages for prejudice suffered but also being at risk of being prosecuted at the criminal level for unlawful personal data processing.[36]

Subsequent rulings from lower courts, following the same rationale, provided further clarification in the field of online archives, reducing those burdens on publishers and owners of the archives. This is what clearly emerges from a ruling decided in February 2014 by the Court of Appeal of Milan enforcing such obligation to keep personal data updated, through the insertion of a link apt to contextualize the news along the evolution of the events, derived from Article 7 of the Italian Data Protection Code, being shaped not as the obligation to update in general any information in the archive, but only upon a precise and specific request of the person concerned[37].

Notwithstanding such clarification, this jurisprudence on online archives cannot be regarded as definitely settled, being on the contrary questioned recently by a problematic ruling adopted again by the Italian Supreme Court – this time in the post *Google Spain* case scenario – perceived as a real threat to the freedom of the press.

II-THE IMPACT OF THE CJEU'S JUDGMENT IN GOOGLE SPAIN ON THE ITALIAN LEGAL SYSTEM.

The *Google Spain* ruling, adopted in May 2014 by the European Court of Justice, clearly had a relevant impact on the Italian legal system, since until that decision courts and the Italian DPA had followed the same position expressed by the Advocate General in that case – the one precisely overturned by the CJEU - namely imposing directly on the source web page publishers the obligation to protect the "right to be forgotten" of individuals through appropriate measures for updating the news, while conceiving search engines as pure intermediaries not liable for personal data processing.

The new scenario brought about by the *Google Spain* judgement recognising search engines as data controllers, with their amounting to entities that individuals can directly turn to, not only for requests of delisting of search results but also, for exercising their "right to be forgotten" as a "right to erasure"

34 See Giovanni De Gregorio and Andrea Serena, 'Online archive and right to be forgotten: from the approach of the Italian Privacy Authority to the last decision of the Italian Supreme Court', (2016) Law and Media Working Paper Series no. 19/2016, 2.
35 A. Di Majo, 'Il tempo siamo noi …', (2012) in Corriere Giuridico, 771; Giusella Finocchiaro, 'Identità personale su Internet: il diritto alla contestualizzazione dell'informazione', in Diritto dell'informazione e dell'informatica, 2012, p. 383 ss.
36 F. Di Ciommo and Roberto Pardolesi, 'Dal diritto all'oblio in Internet alla tutela dell'identità dinamica. È la Rete, bellezza!', (2012) Danno e responsabilità, 704 ss.
37 Court of Appeal of Milan, February 2014, see Marco Bassini, 'La Corte d'appello di Milano sulla contestualizzazione delle notizie diffamatorie sugli archivi online dei giornali', (2014) Diritto dell'informazione e dell'informatica, IV-V, 831.

THE RIGHT TO BE FORGOTTEN IN ITALY

in order for links to relevant pages to be deleted in case personal data reported in the news are no longer relevant (due to the long time passed, or in case of absence of public interest or of an historical concern). This has immediately led to a new perception of search engines as private entities actually displaying a sort of "para-constitutional role"[38], with their being directly involved – as judges are – in balancing conflicting rights.

This new perception is well reflected in the immediate reaction the Italian DPA displayed shortly after the CJEU's decision when, in July 2014, the Authority not only imposed on Google an order to comply with the privacy measures it had set forth to protect Italian users' privacy, but for the first time ever in Europe it actually reinforced such order through the adoption of a verification protocol focused on the practical implementation of such measures by Mountain View. With this, Google could be subject to regular checks by the Italian DPA to monitor progress status of the actions taken to bring its platform into line with domestic legislation by the deadline of 15 January 2016[39]. It is remarkable that the protocol, requiring Google among other measures to put in place a specific timeframe regarding data deletion from both online and back-up systems, foresaw also a continued exchange of information between Mountain View and the Italian DPA regarding Italian users' delisting requests received by Google so as to monitor the implementing arrangements of the right recognised by the CJEU, so allowing a sort of "supervisory" role by the Italian DPA.

As already clarified, in the Italian legal system the solutions already acknowledged for balancing the freedom of information, the right to information, the right to be forgotten and the freedom to exercise free historical research, initially represented by orders for the "de-indexing" of the relevant article from general search engines while leaving it accessible by means of the internal website search function[40] (something that can be accomplished by the source web page publisher independently without requiring the active participation of the search engine service provider), have also been complemented – after the 2012 Italian Supreme Court's ruling – with decisions entailing a direct intervention on the source web page, with orders for updating the concerned piece of news on the newspaper electronic archive to contextualise them by including the subsequent events, occurred upon a specific request.[41]

In any case, both the Italian DPA and lower courts giving specific implementation to the CJEU's decision have reaffirmed that the right to be forgotten has to be weighed against the freedom of the press, excluding such right in case of recent data of public interest.

In deciding an appeal of a user against a Google decision not to de-index an article appearing in Google's search results, reporting an inquiry where the person had been involved in what was regarded by the plaintiff as "extremely misleading and grossly prejudicial", the Italian DPA in a decision enacted in December 2014 made clear – while rejecting the request – that users cannot invoke the right to be forgotten for events not only recent but also having a relevant public interest (like an important judicial enquiry), reporting facts respecting the essentialness of information, but it added that the user can ask the publisher to request a contextualisation of the article, through an integration of the news published.

Furthermore, the Italian DPA stated an important principle regarding the so called "snippets", the texts automatically displayed by Google complementing the search results, entitling those adversely affected to request for their deletion when those snippets were not consistent with the news reported in the web pages the links are referring to, as they are incomplete. This is because such snippets represent processing of personal data and thus they have to be relevant, correct and not misleading.

Again, more recently in another case, the Italian DPA rejected the appeal filed by a former terrorist who, in 2009, having served his sentence, had unsuccessfully asked Google to de-index web pages reporting serious crimes he had committed in the 1970's and 1980's and the removal of search suggestions associating his name with the term "terrorist". The man had thus turned to the Italian DPA invoking the right to be forgotten assuming that he was not a public figure but a free

38 Oreste Pollicino, 'Google rischia di "vestire" un ruolo paracostituzionale', (2014) Il Sole 24 ore, 15 May 2014.

39 Italian DPA, Decision 10 July 2014, no. 3283078; Decision 20 February 2015, The protocol envisaged quarterly updates on progress status and empowers the DPA to carry out on-the-spot checks at Google's US headquarters to verify whether the measures being implemented are in compliance with Italian law. Thus, it enabled the DPA to continuously monitor the changes Google was required to make to the processing of personal data relating to users of its services – including its search engine, emailing, YouTube and social networking services.

40 Alessandro Mantelero, nt. 28.

41 See the orders requiring an updating of the news in the online archive issued by the Italian DPA to one of the main news magazine editor, the "Gruppo Editoriale L'Espresso" : decisions 24 January 2013, no. 31; 23 July 2015, [doc. web n. 4364422].

citizen, harmed in his reputation by the permanence on the web of old news causing a misrepresentation of his actual life. The Italian DPA, in referring also to the 2014 Guidelines enacted by the Art.29 Working Party gathering the European Privacy Authorities, held that no right to be forgotten could be recognised for information concerning serious crimes (an issue the European DPA had agreed upon to be dealt with more stringent evaluations on a case by case level) as all the news reported had gained historical value, almost being part of the collective memory, and still subject to a huge public interest, as demonstrated by the topicality of the references displayed by the same Url[42].

Assuming on the contrary the lack of an actual public interest, the Italian DPA in another recent case upheld the request of an Italian citizen asking for the removal from Yahoo!'s search engine of links to a US website reporting news of an old judicial misadventure that had occurred to him in that country. He argued that the order to remove all links to the content was due to the fact that the news was out of date and not updated with the positive solution of the case[43].

Ultimately, in a very recent case decided in June 2017, the Italian DPA stressed once more that the passing of time is not the only factor to be weighed in recognising a right to be forgotten, as other important limits can derive (as clearly stated in the Article 29 Working Party's Guidelines on the implementation of the *Google Spain* judgment) from the public role vested in the data subject involved and the actual public interest in the news reported, thus paving the way for more nuanced solutions in balancing the conflicting rights at stake[44].

The action had been brought by a top-level public official who had asked for the deletion of some URLs from the list of results displayed when googling his name (these results referred to a criminal case that had occurred 16 years before and ended with a decision against the man, who had subsequently experienced a complete rehabilitation). It is worth considering, in the first instance, that the Italian DPA rejected the arguments raised by the defence of Google, arguing that the results of the research were not technically made only "on the basis of his name" – the condition requested by the *Google Spain* decision for de-listing – as those results appeared only when the name of the claimant was searched together with words such as "sentenced" and not on its own. The Italian DPA clearly stated that it was necessary to take into due consideration all the results of the search obtained on the basis of the name of the data subject, thus encompassing also those results associated with further specifications, such as the role vested, or the circumstances of the criminal judgment.

Upon these criteria, the decision partially upheld the action, since the Italian DPA ordered Google to de-list and remove the URL for the news written in 2001, by virtue of the time passed and the inaccuracy of the information contained therein. However, it also recognised that a public interest prevailed regarding two more articles (published in 2012 and 2016), which were not only recent, but had accurately reported both the criminal sentence and the rehabilitation involving a public person. These were all factors that led the court to recognise as prevailing a right to information, as the news had been reported in a wider context referring also to the institutional role currently played by the data subject, thus justifying an actual public interest in the news.

Along the same lines, based on an inclusive interpretation of the notions of public figure and public role, the first Italian judicial decision on the right to be forgotten after the *Google Spain* case, enacted by the Court of Rome in December 2015,[45] rejected a request raised by a well-known attorney, for de-listing of links referring to a court case dating back to the years 2012/2013. The case was regarding an alleged fraud in which he had been involved together with some representatives of the clergy and other subjects linked to the criminal organisation known as "Banda della Magliana" without later on being convicted, thus leading him to call also for a monetary compensation due to the illegal treatment of his personal data. In recalling the CJEU's judgement rationale, the Court of Rome rejected the plaintiff's request as those news fell under the protection of freedom of expression, assuming that the right to be forgotten could only be granted when news are not recent and when lacking a public interest. For the court, the latter criterion in the context on the right to be forgotten leads to consider as a "public figure" not only politicians, but also businesspersons and lawyers.

III-A RIGHT TO DE-LIST, TO UPDATE OR..... TO 'FORGET' THE NEWS? REFLECTIONS ON A RECENT DECISION BY THE ITALIAN SUPREME COURT.

A recent decision of the Italian Supreme Court[46] seems

42 Italian DPA, Decision 31 March 2016, doc. web n. 4988654.
43 Italian DPA, Decision 15 February 2017.
44 Italian DPA, Decision 15 June 2017, doc. web n. 6692214.
45 Court of Rome, First Division, 3 December 2015, no. 23771.
46 Italian Supreme Court of Cassation, Decision 24 June 2016, no. 13161.

THE RIGHT TO BE FORGOTTEN IN ITALY

to open an unprecedented and problematic path on the grounds of the right to be forgotten, regarding both its extent and balance against the freedom of the press and the right to be informed about news that can be of public interest, calling into question – in the field of online archives – principles that appeared to be deeply consolidated in the Italian legal system.

The case, in fact, did not involve de-listing from the Google search engine, or intermediary liability, nor the updating of news displayed to protect the "actual" true identity of the plaintiff, but it immediately addressed the issue whether the right to be forgotten should prevail over freedom of expression in records included in newspapers' archives.

The case arose from the request of the owners of an Italian restaurant to remove an article published in a local online newspaper, reporting a criminal proceeding regarding their restaurant in 2008. The plaintiffs in 2010 had already asked the publisher to remove the news item and, reacting to his refusal, they filed a lawsuit claiming reputational damages and the violation of their privacy together with the violation of their right to be forgotten. What is striking in this case is that the plaintiffs were not contesting whether the facts reported were true, nor whether there was public interest in the whole story, but rather they filed their law suit simply on the grounds that they did not want that news item to still be accessible on the online archive of the newspaper and indexed by Google's search engine, as it was detrimental to their reputation and to the image of their restaurant.

The first court's decision – released in the pre-*Google Spain* scenario in 2013 – recognised precisely the main argument raised by the plaintiffs, namely that after two and a half years from the events reported - and from when the article had been first published - the right to inform the public could not possibly be considered a legitimate ground to maintain in the online archive the news item as the article had already been kept online for a period considered suitable enough to guarantee the right of the public to be informed. Still, as the publisher in the meanwhile had already deleted the article from the online archive, the court could not order the removal of the article but in any case, it awarded the plaintiffs with significant damages.

The Supreme Court, in a totally surprising way, confirmed the same rationale of the first court's ruling, considering – in a discretionary manner lacking a legal provision in that sense – that after the lapsing of time of two and a half years (which was the time passed from the online publication until the formal request of removal addressed by the owners of the restaurant) and up until when the article had been eventually deleted, an illegal processing of personal data had occurred, motivated by two reasons: the fact that "the news article was easily searchable and accessible" (thus retrievable with Google search function just by typing the name of the plaintiff and of the restaurant) and the "widespread readership of the local online newspaper" provided by its online publication.

So, being that the time passed – two and a half years – was considered sufficient enough to satisfy the public interest, as a guarantee of the right to be informed, at least since that "expiry date" (namely since the date when the formal notice of removal had been received by the publisher) the Court held that those data "could no longer be disclosed". According to the Italian Supreme Court, such conclusion had to be based on Article 11 of the Italian Data Protection Code stating that "data must be kept in a form which allows identification for a period of time not beyond that which is necessary for the purposes for which they were collected".

The decision has been severely criticized for its consequences on freedom of expression both by Italian legal scholars – ironically also noting that news articles now had an expiry date "just like milk, yogurt and a pint of ice cream"[47]- as well as by prominent European newspapers[48] and eventually the World Association of Newspapers and News Publishers[49] who, respectively, argued that the ruling paved the way in the last instance for providing a new meaning of the right to be forgotten as "the right to remove inconvenient journalism" or as "the right to forget the news". These reactions clearly boosted the perceptions of those who had already argued that the right to be forgotten as recognised in Europe could ultimately "corrupt history"[50] or even more harshly assumed that "Europe is exporting censorship all over the world"[51].

47 Guido Scorza, nt. 13. See also the critical comments by Giovanni De Gregorio and Andrea Serena, nt. 33.
48 Athalie Mattews, 'How Italian courts used the right to be forgotten to put an expiry date on news' The Guardian (London, 20 September 2016, as modified on 21 February 2017) <www.theguardian.com/media/2016/sep/20/how-italian-courts-used-the-right-to-be-forgotten-to-put-an-expiry-date-on-news> accessed 26 March 2017.
49 Elena Perotti, 'The transformation of Right to be Forgotten into Right to Forget the News' WAN-IFRA Blog (22 July 2016) <blog.wan-ifra.org/2016/07/22/the-transformation-of-right-to-be-forgotten-into-right-to-forget-the-news> accessed 26 March 2017.
50 Edison Lanza, 'Freedom of Expression Rapporteur of the Inter-American Commission on Human Rights, WS 142 Cases on the Right to be Forgotten, What Have we Learned?', Internet Governance Forum 2015.
51 Geoffrey King, 'EU"Right to be Forgotten" Ruling Will Corrupt

It is worth noting that this decision is not isolated among courts in Europe, as it appears to reflect the same reasoning underlying a decision, two months earlier, adopted by the Belgian Cour de Cassation (the highest Belgian tribunal) in the Le Soir case[52]: Here, the newspaper "Le Soir", having made freely available online its entire archive since 2008, had been ordered to modify an article that had been published 22 years before, with the anonymization of the applicant's name in the online version of the original article (in the said article, published in 1994, a car accident causing the death of two people had been reported together with the citation of the driver's full name, who therefore asked the newspaper to remove the article or anonymize it).

What is even more worrying in the Italian Supreme Court's judgement is that, contrary to the Belgian one where the facts at stake had occurred decades in advance, the case originating the decision was still at bar. So, neither the fact that the events reported were recent, nor the fact that highly sensitive data were under issue, since they included criminal charges, were duly taken into consideration by the Italian Supreme Court. On the contrary, it recognised the "absolute supremacy" of the right to be forgotten of the plaintiffs, thus recasting completely the terms of the issue, as it is no longer clear which is the rule and which is the exception.

Even if the impact of this judgment on future case law is still to be assessed (though, for the time being, a chilling effect cannot be excluded, as publishers may be led to consider seriously all takedown notices also removing articles still relevant for the public), this decision is to be wholly criticised for, on the one side, being built on a wrong pre-comprehension severely affecting online journalism and, on the other side, departing from the balancing test made clear at the supranational level.

To begin with, the Italian Supreme Court's decision has made even more evident an issue, which is still not completely settled, in the Italian case law. The decision, in fact, moves from a distinction between online publication and paper publication as it links the illegal data processing to the keeping of the direct and easy access to the news article and to its dissemination through the web, which – contrary to the paper version of the same newspaper – are interpreted as leading, within a short period of time, to the fading of public interest in the news item. Actually, it was precisely on this rationale that a former lower regional court's decision in 2013, in granting the recognition of the right to be forgotten, had ordered the online archived article to be deleted, while on the contrary considering the storage of a single paper copy appropriate.[53]

Here, again, the Supreme Court equates the keeping of the news item in an online archive to a permanent publication. This conclusion cannot be retained, as on the contrary the different notions of mere conservation of a news article in an online archive and the publication of the said article, even if on the newspaper website, are to be traced. The publication, in fact, consists in an offer to the public of a certain product for its dissemination and only to such publication a right to be forgotten can be recognised, in case the news item has infringed the principles of truthfulness, continence and relevance. On the contrary, as already accomplished in 2014 by the Court of Appeal of the same regional court previously mentioned,[54] the insertion of an article in an online archive, while enhancing the access to its content, cannot be considered as a new publication being only equivalent to the physical access to the article (the online publication actually becoming relevant for defining higher amounts of damages in cases of defamation,[55] due to the increased prejudice suffered caused by the capillarity of an online publication). One might argue, on the contrary, that the conservation of a news item in an online archive is something similar to an archiving operation, which follows different rules, as the processing of personal data for historical purposes may be carried out also upon expiry of the period that is necessary for achieving the different purposes for which the data had been previously collected or processed (see in the Italian Data Protection Code, Article 99).

Now, both decisions adopted in 2016 by the Italian and Belgian Supreme Courts, quite surprisingly made specific reference, in their legal reasoning, to the *Google Spain* judgement to reach the conclusion that the right to privacy, embedding the right to be forgotten, should prevail over the freedom of expression justifying the removal of the news article from the online archive. But that conclusion is clearly based on a severe misunderstanding of *Google Spain*'s reasoning, which is not about "deleting content" and

History', Committee to Protect Journalists (CPJ) Blog, June 4, 2014, <cpj.org/blog/2014/06/eu-right-to-be-forgotten-ruling-willcorrupt-histo.php.>, 23, accessed 1 May 2017.

52 See *P.H. v. O.G.,* C.15.0052.F (Belgian Supreme Court [Cour de Cassation], 29 April, <www.juricaf.org/arret/BELGIQUE-COURDECASSATION-20160429-C150052F> (French only).

53 Court of Milan, First Civil Section, decision 26 April 2013, no. 5820.

54 See nt. 36.

55 Giovanni De Gregorio and Andrea Serena, nt. 33.

information from the Internet, as it merely recognises, after the passing of a reasonably long time (in *Google Spain* the time passed amounted to 16 years), a right to de-listing the links. Thus, a "right not to be seen/found" only affecting the results gathered from searches made when typing the person's name and only provided that the person at stake does not fulfil a public role. The CJEU's judgement, moreover, clearly mentioned an exception for "journalistic purposes" and expressly stated that the right to be forgotten cannot be exercised against the publisher of the webpage if the processing is carried out "solely for journalistic purposes" (par. 85), something which on the contrary precisely was enforced in the Italian case.

The Italian Supreme Court's decision seems to have shaped a right to be forgotten as a sort of "absolute right of informational self-determination" and, even more alarming, empowering de facto individuals who feature in a news story "to decide when the time has come to remove that story from the collective memory".[56] Like a Leibnitzian monad, the right stemming from the approach followed by the Italian Supreme Court's decision is solely built on the amount of time passed since the occurrence of the relevant facts, without any confrontation with the wider "world of balancing criteria" the European Data Protection Authorities, gathered in the Art. 29 Working Party, carefully defined in the "Guidelines" adopted in November 2014 for the implementation of the *Google Spain's* judgement; precisely built to be read in the light of "the interest of the general public in having access to information".[57] Those criteria, inevitably leading to the granting of a right to de-listing, through a case-by-case approach, embrace a very wide scenario of relevant circumstances – thus justifying the Art.29 WP's conclusions. Namely, that the impact of de-listing on freedom of expression and access to information would have been very limited[58] – ranging from subjective criteria (referring to the data subject, whether public figure or playing a public role or a minor), to objective criteria (regarding the type of data processed, whether accurate, relevant, not excessive, sensitive data or referring to criminal charges), criteria referring to the consequential effects (prejudice/impact disproportionate, risks for the data subject) and eventually to criteria referred to the modality or the context of the publication (among these, the publication in the context of journalistic purposes).[59]

Moreover it is to be stressed that with this ruling the Italian Supreme Court seems to have disregarded the duty of consistent interpretation with the Strasbourg Court's jurisprudence stated by the Italian Constitutional Court in its decisions no. 239 of 2009 and 49 of 2015, the latter of which has better clarified that Italian courts are bound by a Strasbourg's decision if it: a) decides precisely on the same case which is brought again before the Italian judge; b) is part of a well-established and consistent thread of European case law; c) is a pilot judgment.[60]

Now, on the subject matter of online archives, in 2013 the European Court of Human Rights issued an important decision in the case Węgrzynowski and Smolczewski v. Poland[61] that can be regarded as a direct precedent, as it dealt with the question of deleting content violating privacy from Internet archives. In this ruling – one of those decisions reflecting the ever growing ECtHR self-perception of its own role as evolving into a peculiar European constitutional court[62] – the ECtHR stressed that, although the Internet publications may generate a particular risk for the protection of private life, the Internet archives serve the public interest and are subject to the guarantees arising from the protection of freedom of expression (art. 10 ECHR) as they make a substantial contribution to preserving and making available news and information and they constitute an important source for educational and historical research (§ 59). While reminding that "it is not the role of judicial authorities to engage in rewriting history by ordering the removal from the public domain of all traces of publications which have in past been found, by judicial decisions, to amount to unjustified attack on individual reputations", the ECtHR acknowledged however, that "it would be desirable to add a comment

56 See Guido Scorza, nt. 13.
57 See Article 29 Data Protection Working Party, 'Guidelines on the Implementation of the CJEU Judgment on Google Spain v. Costeja', 14/EN WP 225 (November 26, 2014) available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/ wp225_ en.pdf, accessed 27 April 2017.
58 See Guidelines, nt. 55, 11.
59 See Andrea Turturro, 'Il "quasi oblio" in azione, (2015) Dir. Soc, 443.
60 See on this jurisprudence Diletta Tega, 'A National Narrative: The Constitution's Axiological Prevalence on the ECHR–A Comment on the Italian Constitutional Court Judgment No. 49/2015', Int'l J. Const. L. Blog, May 1, 2015, <www.iconnectblog.com/2015/04/mini-symposium-on-cc-judgment-49-2015> accessed 27 April 2017.
61 ECtHR judgment from 16 July 2013 *Węgrzynowski and Smolczewski v. Poland* (application no. 33846/07).
62 Guido Raimondi, the Vice-President of the ECtHR, said that the Court rules on single cases, but also feel as if playing a constitutional role, see 'Corte di Strasburgo e Stati: dialoghi non sempre facili. Intervista a cura di Diletta Tega a Guido Raimondi', Quaderni costituzionali, (2014), 468; in the same perspective, see the memoir of a well-known former President of the Court, J.P. Costa, 'La Cour européenne des droits de l'homme. Des juges pour la liberté', Paris, (2013)

to the article on the website informing the public of the outcome of the civil proceedings in which the courts had allowed the applicants' claim for the protection of their personal rights" (§ 65).

Contrary to the precedents from the ECtHR and the CJEU, the Italian Supreme Court's decision in 2016 chose an "absolutist" understanding of the right to be forgotten, through the removal of the information from the online archives, at the expense of competing rights of freedom of expression and the interest of the public to have access to the information. On the contrary, if it had followed the supranational case-law, the Italian Supreme Court would have been able to precisely meet the goal the Italian Constitutional Court requires from national courts when applying the said case-law, namely that

> national authorities have a duty to prevent the protection of certain fundamental rights – including from the general and unitary perspective of Article 2 of the Constitution – from developing in an unbalanced manner to the detriment of other rights also protected by the Constitution' (emphasis added).[63]

IV-FINAL COMMENTS.

In the aftermath of the landmark decision in *Google Spain*, in the Italian legal system lights and shadows seem to accompany the newly emerging right to be forgotten in the online environment. While lower courts and the Italian Data Protection Authority have been heavily committed to trying to further clarify and reinforce the necessary balance between personal privacy interest and public interest in freedom of expression and access to information along the lines of the CJEU's test in *Google Spain*, the latest Supreme Court case-law showed misperceptions regarding the extent of the right to be forgotten as regarding online archives.

In this regard, it might not be useless to stress that the said misperceptions might have been overcome if only the Italian court had referred the issue to the CJEU, as it did in a previous case in 2015, the Manni case,[64] thus leading the CJEU to provide it with more clarity on the right to be forgotten[65]. Thus, in the very recent ruling in Manni, where the relationship between the availability of personal data in public registers and the data subject's right to limit this regime of full disclosure was at stake, the CJEU clearly reaffirmed that the right to be forgotten is not "absolute". This is because it always needs to be balanced against other fundamental rights (in this case, as said, it was not the freedom of expression but the interests of third parties to gain information on particular persons holding a key position in the economic life that was at stake[66]), requiring a case-by-case assessment taking into account the type of information, its sensitivity for the individual's private life, as well as the interest of the public in having access to that information, and the role played by the data subject.

In any case, these misperceptions presumably will be solved once the new General Data Protection Regulation[67] enters into force in May 2018, not only due to the provisions contained in Articles 17 and 18, replacing and better qualifying the provisions contained in the Data Protection Directive on erasure and blocking of data, but also because these new provisions, by virtue of their being inserted in a regulation, will be directly applicable within the Member States legal frameworks thus providing for a higher degree of data protection harmonisation within the European Union.

In fact, it should not be underestimated that under Article 17 the right to erasure – even if labelled in this piece of legislation also as a "right to be forgotten" for political reasons to mark a distinction from the US legal tradition[68]– has been framed with specific limits precisely aiming at encompassing reinforced safeguards for freedom of expression, along with a broader extent of the "media exception"[69]. Seen from

63 Italian Constitutional Court Decision no. 317/2009.

64 CJEU, Request for a preliminary ruling from the Corte suprema di cassazione (Italy) lodged on 23 July 2015, Case C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*.

65 For a thorough understanding of the case, see Alessandro Mantelero, 'Right to be forgotten and public registers. A request to the European Court of Justice for a preliminary ruling' in EDPL - European Data Protection Law Review, 2016/2

66 Case C-398/15 (CJEU, 9 March 2017). The CJEU, following the Opinion of the AG Bot, clearly stated that no anonymization, deletion or blockage of the personal data contained in a Company Register could be allowed, considering that, there is a prevailing public interest in the transparency, legal certainty and good functioning of markets, which the completeness of the Company Register's records contributes to achieve.

67 Regulation (EU) 2016/679 of the European Parliament and of The Council of 27 April 2016.

68 See Franco Pizzetti, nt.1.

69 Giancarlo Frosio, 'Right to Be Forgotten: Much Ado About Nothing' (January 31, 2017). 15(2) Colorado Technology Law Journal (2017 Forthcoming), available at SSRN: <https://ssrn.com/abstract=2908993>, last accessed 1 May 2017 notes (pp. 9-10) that 'the "media exception" of the GDPR appears substantially broader than its equivalent in the earlier Data Protection Directive. The exception is no longer limited to data processing "carried out solely for journalistic purposes or the purpose of artistic or literary expression." Rather, the exception aims more generally to reconcile

THE RIGHT TO BE FORGOTTEN IN ITALY

the Italian perspective, what is striking to stress is that Article 17 expressly states that a right to erasure – a right a data subject might exercise mainly when "personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed" – cannot be granted against controllers if they are "exercising the right of freedom of expression and information" or if the personal data processing is necessary "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" in so far the right to be forgotten "is likely to render impossible or seriously impair the achievement of the objectives of that processing." (Art. 17, par. 3, GDPR).

Particularly useful, for a more gradual approach in balancing the contrasting rights and interests at stake, should also turn out to be the new "right to restriction of processing", provided by Article 18, to be invoked when the data subject wants to contest the accuracy of personal data processed, thus pre-emptively restricting access to the news item pending the examination of its accuracy (with data controllers entitled only to store the personal data, but not further process it), and to be lifted in short time, i.e. as soon as such verification by data controllers is performed.

In the meanwhile, the GDPR will come to a practical application and, for the Italian legal system, the solution that the CJEU will provide in the preliminary reference raised on February 24, 2017, by the French highest administrative court (the "Conseil d'Etat") will be of the highest importance.

In this request for a preliminary ruling, serious issues have been raised in the light of the European Court of Justice's judgment in its Google Spain case, precisely

> "in relation with the obligations applying to the operator of a search engine with regard to web pages that contain sensitive data, when collecting and processing such information is illegal or very narrowly framed by legislation, on the grounds of its content relating to sexual orientations, political, religious or philosophical opinions, criminal offences convictions or safety measures."[70]

data protection rights with "the right to freedom of expression and information, including the processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression."

70 See Conseil d'Etat, Press Release 24 February 2017.

THE DIGITAL RIGHT TO BE FORGOTTEN IN SWEDEN: THE THEORY AND PRACTICE OF PRIVACY PROTECTION MECHANISMS IN THE FACE OF REFERENCING BY SEARCH ENGINES

By Patricia Jonason
Associate Professor, Södertörn University

Google Inc has received 54,038 requests to dereference Swedish URLs since the judgement of the Court of Justice of the European Union, C-131/12 *Costeja*.[1] After examining these requests, Google removed 43.7% of the search results (i.e. 23,613 URLs) but refused to dereference in 56.3% of cases (i.e. 30,425 URLs).[2] In other words, Google refused to grant the dereferencing requests in a little over half of the cases, which corresponds to the average recorded by the American Internet search engine across all European countries.[3] What kind of help from public authorities may individuals to whom a request for delisting has been denied by the operator of a search engine have at their disposal? In other words, how do the Swedish authorities apply the Google ruling? These are the questions tackled in this paper, first focusing on the manner the Data Protection Authority, the Datainspektion (DI), deals with the issue, then looking at how the courts handle complaints against a search engine operator's decision not to delist an incriminated URL.

I-INTRODUCTION

The starting point is twofold. Firstly, Article 12 of the Data Protection Directive 95/46/EC[4] places Member States under the obligation to guarantee *"every data subject the right to obtain from the controller [...]the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive"*. Secondly the Court of Justice of the European Union stated in the *Costeja* case that *"where the controller does not grant the request, the data subject may bring the matter before the supervisory authority or the judicial authority so that it carries out the necessary checks and orders the controller to take specific measures accordingly."*[5] The said measures can involve, *"ordering the search engine operator to remove, from the list of results displayed following a search made on the basis of a person's name, links to web pages published by third parties containing information relating to that person."*[6] It follows that the national law is expected to set up mechanisms to effectively implement the right to dereferencing.

How does the Swedish Data Protection Authority, the Datainspektion (DI), perform its task of protecting individuals with respect to referencing? (II). What is the position and the powers of Swedish courts in this area? (III)

This analysis will lead us to consider questions relating to the practice of these authorities, as we will consider actual cases of requests for dereferencing. We shall then also consider procedural issues and particularly the question of the effectiveness of Swedish procedural rules with regards to the requirements of European law. The intrinsic question tackled by this paper is the one of the application in the Swedish context of the right of the citizens to have their data protected, here through the right to be forgotten.

Une version française de cet article est accessible à : https://blogdroiteuropeen.files.wordpress.com/2017/05/article-patricia-ok.pdf

1. Judgment of the Court (Grand Chamber) of 13 May 2014 (request for a preliminary ruling by l'Audiencia Nacional - Spain) – *Google Spain SL, Google Inc. / Agencia de Protección de Datos (AEPD), Mario Costeja González*

2. In all, in October 2017 Google had agreed to dereference 816,396 URL (43.2%) refused to dereference 1,074,701 (56.8%).

3. https://transparencyreport.google.com/eu-privacy/overview?delisted_urls=start:1401235200000;end:1506902400000&lu=delisted_urls (2 October 2017).

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.

5 Point 77

6 Point 82

THE RIGHT TO BE FORGOTTEN IN SWEDEN

II-THE RIGHT TO DEREFERENCING AND THE CONTROLLING BODY, THE DATAINSPEKTION

The Swedish Data Protection Authority the Datainspektion, is in the front line when it comes to implementing the *Costeja* decision. This body, which was set up by the Data Protection Act (the personuppgiftslagen or PuL (1998:204))[7], is chiefly responsible for "supporting" people when they ask for websites which contain information on them to be deindexed. This involves either informing data subjects of their rights and the necessary procedures (A) or, if the Internet search engine operator rejects their requests for dereferencing, employing the whole panoply of legal powers granted by the Personal Data Act (B). This Authority also has the general task of *"monitoring the application"*[8] of the national law on personal data in order to perform more general checks on how those who are responsible for processing (including Internet search engine operators) satisfy their obligations (C).

A-A task to provide information

The Datainspektion works *"to protect people's privacy against interference from personal data processing"*[9] and one of its tasks is to inform the people who are responsible for processing (data controllers) and the people affected (data subjects) of the rules which apply to the processing of personal data. However, it is not easy for a net user visiting the Swedish Data Protection Authority's website to find immediate and coherent information on his or her different rights concerning dereferencing in relation to the right to be forgotten, including what action the Datainspektion can take. In fact, the question of the right to dereferencing/right to be forgotten is not particularly conspicuous on the site at the present time (unlike questions concerning social networks, video surveillance, the iCloud or processing of personal data by employers, which are all given special treatment). The only way to obtain information on this subject on the Datainspektion's website is to perform a search using keywords such as "the right to be forgotten" on the site's search engine. The Internet user will then discover that the Datainspektion performed an audit of Google in May 2015.[10]

The Internet user will also find a page containing more operative content entitled *"remove the search results connected to your name from Internet search engines"*,[11] which briefly explains in simple terms that it is now possible for Internet users to delete information which they may come across when performing searches with their own names on Google or Bing.

The DI precises furthermore that it was the European Union that, in 2014, decided that everyone had the right to do this if search results were incorrect, no longer relevant or excessive. Two dereferencing forms, one from Google, the other from Microsoft (for its Bing search engine), with explanations from these search engine operators on how to implement these procedures, are also accessible on the same webpage of the DI.

The Datainspektion intends, in the meantime, to provide more information on the issue of dereferencing in the short or medium term. Thus, a web page entitled *"Right to erasure"*[12] aiming at providing information on the right to erasure as laid down in the General Data Protection Regulation[13] will be completed on an ad hoc basis, particularly by providing guidelines to specific groups.[14]

However, nowhere is it mentioned that an individual whose complaint has been rejected by an Internet search engine operator has the right to make a complaint with the Datainspektion under the right to be forgotten, nor does it mention the need to contact the operator first before contacting the Data Protection Authority. Information on the complaint procedure is indeed obtained from the *"about the DI"* scroll down menu, where an explanation of how the complaints system works is given under the *"working method"* caption.[15] Moreover, it is stressed that although the Authority receives a number of complaints every day, it is under no obligation to perform an inspection following a complaint, and it is not obliged to act as the complainant's representative.

7 Originally by the Data Act, datalagen, from 1973.
8 Article 28.1 of the Directive 95/46/EC.
9 Swedish decree (2007:9758) concerning the Datainspektion
10 Procedure which we shall return to, see infra.

11 *Ta bort sökträffar på ditt namn från sökmotorer*, http://www.datainspektionen.se/lagar-och- regler/personuppgiftslagen/publicering-pa-internet/ta-bort-soktraffar-pa-ditt-namn-fran-sokmotorer
12 *Rätten till radering.*
13 Regulation (UE) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
14 http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/de-registrerades-rattigheter/ratt-till-radering/.
15 The complaints which are not explicitly referred to in the Swedish Personal Data Act, converts to what exists in the French Data Protection Law, are one of a number of elements which the DI can use to initiate an individual or general control procedure.

THE RIGHT TO BE FORGOTTEN IN SWEDEN

The DI received nevertheless a certain number of complaints against refusals to de-index and began a procedure against the Internet search engine operator Google, requiring it to re-examine a number of rejected dereferencing requests. The complaints considered also prompted the Datainspektion to carry out a general inspection of this operator to assess its procedures for dealing with deindexing requests. The Datainspektion therefore started a dual procedure. Although both facets of the proceedings are interconnected and were started simultaneously, they are considered separately in the following.

B-Processing individual complaints

The DI received an average of one complaint a week concerning dereferencing requests after the European Court's judgment and the resulting dereferencing request procedure became public knowledge. The DI selected 13 complaints out of the hundred received, which it sent by post to Google Sweden and Google Inc on 27 May 2015 to be examined by them.

Some of the complaints were chosen because they were representative of all the complaints and others because of their specific nature. The decision to investigate these cases was not taken exclusively in order to settle individual complaints, but also, to evaluate Google's procedures; notably, how it has applied and is applying the criteria laid down by the ECJ in the *Costeja* judgment.

The notification the DI sent to Google asked the search engine operator to inform it of the following for each complaint, 1) the documents Google used to make its assessment, 2) the question whether Google had "documented" the content of the sites which the complainant wanted removed, 3) whether Google was standing by its refusal to dereference and the reasons for the refusal.[16]Only the parent company, Google Inc replied to the notification[17] on 30 September 2015, stating that its Swedish subsidiary did not have control of the webcrawler software or the ability to access Google's search index or to modify the search results.

Out of the 13 complaints transmitted by the DI and re-examined by Google, five resulted in a blockage of all or some of the sites for which the dereferencing request had been made. In some cases, Google was unable to find the incriminated information which appears to have been removed from the identified sites. However, in the majority of cases, Google did not comply with the dereferencing request.

In certain cases, Google based its refusal to dereference on the argument that the incriminated information related to the complainant's professional life and that the legitimate interests of potential customers or business partners prevailed over the complainant's interests. This was the case for a website which included information on a psychiatrist who had been accused of sexually exploiting a person in a position of dependency i.e. a patient to whom he had offered strong beer (Sic) during a therapy session.[18] This was also the case for a website which included information on the reorganisation of a company where the complainant was its Chairman and Chief Executive.[19] Another case concerned a request to takedown a site which contained information detailing how 80 people had laid complaints for fraud against the complainant who been the Chairman and Chief Executive of an estate agency.[20] The last case involved links to websites which contained information on a police officer who had worked in the Internal Investigations Department of the national police (rikspolisstyrelsen). The incriminated information referred to the fact that the policeman was accused of sending offensive letters and half anonymous threats.[21]

In the other cases, Google refused to dereference because of the polemical and and/or political nature of the information involved and also because information concerned the public role played by the complainant. Thus, neither sites containing political attacks against a person who had been involved in creating a national federation for unaccompanied migrant minors,[22] nor sites which reported criticisms of actions by people connected to a critized oil company,[23] were de-indexed.[24]

16 The DI was referring to article 43 of the Personal Data Act which gives it the right, *"for its supervision to obtain on request*
a) access to the personal data that is processed,
b) information about and documentation of the processing of personal data and security of
this processing, and
c) access to those premises linked to the processing of personal data".
17 The company should have delivered its decision on 31st August 2015 but obtained an extension.
18 Annex 3 of Google's letter in reply to the Datainspektion.
19 Annex 8
20 Annex 9
21 Annex 11
22 Annex 5
23 Annex 7:3. This involves a Swedish company which was suspected of having been involved in human rights violations.
24 It is noted that the removal of links containing information on the company itself, a legal person, such as a report on the activities of the Swedish oil company in the Sudan was refused for the reason that the incriminated information did not

In other cases, it was in the public's interest to be informed of the criminal acts committed by the complainant, which was the basis for Google's refusal to dereference the sites, such as sites containing information on the complaint's conviction and prison sentence for rape, aggravated offences against women, ill-treatment and assault committed in 2008.[25] A case which concerned criminal offences but which Google dealt with from the angle of the accuracy of data, involved the results which were obtained when the complainant's name was entered on the Lexbase website, a website containing a database of criminal convictions of people registered in Sweden.[26] Google informed the Data Protection Authority, that the reason for not de-indexing was that access to correct information must be considered to be a principle in the public interest.

In another case, Google refused the complainant's demand to block a search result containing information concerning someone with the *same name* accused of criminal acts, because the incriminated website did not contain information related to the complainant himself.[27]

It appears that the sites which were blocked by Google, were blocked because they contained protected data, and concerned people occupying the position of a judge (in Court or the Public Prosecution Department),[28] or police,[29] or because it was information with an offensive content.[30]

The Datainspektion gave its decision on 2 May 2017[31] after having carefully examined each case in order to assess the context of each of the complaints and to decide whether Google's persistent refusal to deindex the incriminated websites had breached the data protection legislation.[32] The Swedish Data Protection Authority reached different conclusions from the search engine operator concerning five complaints; 1) concerning the complaint by the psychiatrist, the Swedish Data Protection Authority, whilst acknowledging that as the complainant has a certain public role he must accept his professional conduct being open to inspection, criticised the incriminated forum link, stating that the case was dismissed against the complainant at first and second instance and that the forum link charted out the complainant's private life;[33] 2) The Datainspektion also questioned Google's repeated refusal to perform the dereferencing requested by the co-founder of a national federation for unaccompanied migrant minors. From what the DI could ascertain, the incriminated links contain a great deal of private information (including photographs of the complainant's relatives) which is neither relevant nor appropriate with regards to the criticisms levelled at the complainant in her capacity as the representative of an association;[34] 3) The DI also concluded that there was a need for deindexation in the case of a person accused of fraud, arguing that the information contained on the incriminated websites, which related to legal proceedings and the complainant's conviction, was sensitive information concerning facts which were over 10 years old and also, that the complainant had declared that the suspicions of fraud had not led to any conviction;[35] 4) In the case where the complainant had been convicted of several offences (including rape), the Datainspektion criticised Google's refusal to deindex the incriminated sites by highlighting the sensitivity of the conviction data and the fact that the offences were committed a long time ago.[36] 5) In the fifth case, involving a judge, the Datainspektion established that one of the websites which had been "deindexed" by Google was continuing to appear in the search results with information, *"which was probably aimed to outrage"* the complainant (such as accusations of treason and paedophilia) and which were totally inappropriate with respect to the criticisms concerning the complainant's performance of his public office. Thus, in over a third of the cases,

concern a physical person, Annex 7:4.
25 Annex 10
26 Annex 13
27 Annex 12
28 Annexes 6 and 14
29 Annex 11
30 Annex 7:2
31 Decision of 2 May 2017, n° 1013-2015, Tillsyn enligt personuppgifstlagen (1998:204) – Google Inc. och Google Sweden AB. The decision covers a total of 40 pages slightly less than half of which are devoted to individual complaints whilst the other half concerns the general inspection procedure.
32 The Datainspektion considered that the processing used by Google corresponds to the processing stipulated in article 5 a) of the Personal Data Act, i.e. the processing of personal data *"which is not included nor intended to be included in a collection of personal data which has been structured in order of facilitating the search or the compilation of personal data"*. This type of processing is exempt from the majority of the provisions in the Personal Data Act (notably the provisions on the lawfulness of processing, on sensitive data, on the obligation to rectify data). However, such processing is prohibited if it entails an infringement of the privacy of the data subject.
Concerning this "abuse centred model" (compared to the regulatory model") inserted into the Swedish Personal Data Act in 2007, see Blanc-Gonnet Jonason, Patricia, *Vers une meilleure adaptation du droit de la protection des données personnelles à la réalité informationnelle: les exemples français et suédois*, Actualité juridique - édition droit administratif, N° 38, 2008, pp. 2105-2108.
33 See the DI's decision, p. 25
34 The DI's decision, p. 27.
35 The DI's decision, p. 32.
36 DI's decision, p. 35.

THE RIGHT TO BE FORGOTTEN IN SWEDEN

the Datainspektion came to the conclusion that Google had violated the Data Protection Law and ordered it to put an end to the incriminated processing by 2 August 2017. The DI's decision gave information on appealing. Google lodged an appeal within the three-week period for appealing. The Swedish lawyer instructed by Google Inc filed extremely detailed submissions at the Stockholm Administrative Court.[37]

C-The General Inspection Procedure

As mentioned above, in response to the complaints received against operators of Internet search engines, the DI, jointly and simultaneously with the requests to re-examine 13 individual complaints, also began a General Inspection Procedure of the way Google handles the dereferencing requests it receives. Google was asked to provide a general description of how it processes complaints and to answer a number of questions from the Swedish Data Protection Authority.

Apart from a question on the role and function of Google Inc's subsidiary, Google Sweden AB, the Datainspektion specifically questioned Google about the evidence it requires from complainants to establish the infringement of their privacy, which they are claiming to be victims of. The Swedish Data Protection Authority was particularly interested in the question of whether Google required that complainants send it an extract of their criminal record to prove that the information on criminal convictions was no longer current.

The Datainspektion also questioned Google about the length of time it keeps the documents which the people concerned send to it in support of their complaints. The DI asked the Internet search operator whether it had changed its attitude/practice and how, since its reply to the Article 29 Data Protection Working Party on 31 July 2014. Finally, the Swedish Data Protection Authority asked Google to send it the internal guidelines of the American group on processing complaints insofar as such guidelines existed.

The California-based search engine operator[38] explained, in the letter sent in reply to the Datainspektion on 30 September 2015, that it had modified its de-indexing procedure on several occasions after the judgement C-131/12 in May 2014, stating that this procedure is permanently developing.

Google began by briefly describing the procedures implemented by the Google removals teams.[39] If the request to dereference is refused, a succinct explanation of the reasons why is given. Google explains that for reasons of "transparency", webmasters hosting websites which have been de-indexed by Google are informed of the dereferencing without the names of the people affected by the de-indexing requests being given.

Google's reply to the Swedish Data Protection Authority then explains the information the complainant must enter onto the electronic and complaint form.[40][41]

Concerning the Datainspektion's specific question on the documents which Google requests from the complainant to accompany their dereferencing request, Google explains that it asks for additional information if the information given to it on the electronic form is insufficient to examine the request. If the information is incomplete, Google generally refuses to follow up the de-indexing request. Google states that with respect to information on convictions, it may ask the complainant to provide evidence to corroborate the incorrect or outdated nature of the disputed information. In general, Google does not require an extract of the person's criminal record but the complainant may decide to supply this document. Google explains that

37 The lawyer devotes 13 of his 50 page submission (to which 30 annexes are added) to the Order to dereference websites concerning a person suspected of fraud (see 3 above). The lawyer argues that the DI incorrectly balances the interests involved and argues that the Swedish Data Protection Authority has infringed the protection against censorship under the fundamental law on the freedom of expression by requiring the search engine to dereference search results relating to an article in the press. This first procedure by an administrative court is ongoing.

38 Which it must be remembered was the only one to agree to reply to the Swedish authority's request for explanations, see supra.

39 When assessing the complaints which are sent to it, Google considers whether the search results include information which is no longer relevant or which is incorrect and also whether there is an interest in the incriminated information enduring, for example if the information concerns financial fraud, professional negligence, convictions or if the actions involved were performed by people acting in their capacity as public officials (whether elected or not).

40 This is the name which is used to perform the search leading to the incriminated result, the complainant's full legal name, the indication of the capacity of the person making the request if he or she is not the data subject (parent, legal adviser) and a contact email address.

41 The complainant must provide the incriminated URL for each of the results implicated. For questions concerning photographs the complaint must also indicate the terms used to make the research. The complainant must also specify the relationship which exists between him or her and each of the disputed links as well as the reason why including these links in the list of results is no longer relevant, outdated or contestable for a different reason. To finish the complainant must certify that the information contained in the complaint is true and write the date in the "signed on today's date" box".

since the receipt of the Datainspektion's letter notifying the start of the control procedure it has changed its policy for processing complaints on this point and that it no longer *"demands additional documentation from the complainant to clarify their request in this type of case"*.[42]

In reply to the DI's question, concerning the conservation of the documents which are used as support for examining the complaints sent to it, Google explains that it keeps the information provided for 10 years. The documents produced (identity document, judicial documents) are usually destroyed within 25 days of the closure of the dossier, unless legal proceedings are started.

Google, in reply to the Datainspektion's request, explains how it has modified its procedure for processing complaints since it replied to the Article 29 Data Protection Working Party in July 2014. The search engine operator states that it no longer informs webmasters of the deindexation of sites when they contain obvious cases of sexual content which has been published without consent.

Google now systematically displays information that certain results have been de-indexed when the search engine recognises that the search contains the name of a person.

Google also explains that the period for processing complaints is usually five days (which can vary depending on the number of complaints received) and states that it informed each European Data Protection Authority of the procedure it has set up to receive specific dereferencing requests from these authorities, in an email dated 22 October 2014.

The Datainspektion's decision, dated 2 May 2017, makes detailed comments on the information and answers provided by Google, and makes two recommendations to the Internet search engine operator. Firstly, the DI recommends that when Google investigates a request for dereferencing it should *"take all necessary measures so it can examine vague and incomplete requests to remove search results"*.[43] Secondly, concerning the information which Google sends to the Webmaster about the de-indexation of the sites it is hosting, the DI recommends that Google *"only transmits information to Webmasters when it has established that such a communication will not infringe the privacy of the data subject"*.[44] In addition, the Datainspektion which like the French Data Protection Authority (CNIL), is lobbying for global dereferencing,[45] enjoins Google to *"remove the results which can be seen following searches which are made on the data subject's name by people using the Google search engine in countries other than Sweden when it transpires that these search results have such a connection with Sweden and the data subject that they infringe the person's privacy"*.[46] Thus, the American search engine operator has not escaped the Datainspektion's criticisms, with the most crucial point being the issue of the geographical range of dereferencing. This is also a point which Google's lawyer spent a long time dealing with in his submissions, following an appeal against the DI's decision.[47]

III-THE RIGHT TO DEREFERENCING AND THE COURTS

There have been two cases in Sweden, where the people whose requests to dereference websites containing personal information about them were rejected by Google, which have gone to court. One of the cases was settled out of court, whilst the other was the subject of judicial proceedings. In this case, which will be examined in detail here, the Stockholm Court of first instance, found in Google's favour in a judgment dated 9 May 2016[48] by refusing to dereference certain links, ordering the complainant to pay costs of 369,000 Swedish kronor (i.e. the equivalent of €37,000) including 345,000 kronor as defence costs.[49] The court considered that the large amount of the sums awarded

42 Reply from Google, p. 3.
43 Decision of the DI pp. 11-13.
44 Decision of the DI pp. 19-20.
45 The Datainspektion which makes a particularly in-depth legal analysis on this point refers to the French Data Protection Authority (the CNIL) decision of 10 March 2016 concerning Google dereferencing all the domain name extensions for its search engine.
46 Decision of the DI pp.13-18.
47 Google is asking the court to cancel the dereferencing order concerning removals outside the EU/ EEE territory. The Swedish lawyer in arguments in over 30 pages drawn from the case law of international courts (ECJ, ECtHR, the international court of justice), national courts (Canadian, Portuguese, Spanish, American), foreign doctrine notably French and a multitude of legal instruments (ECHR, Charter of fundamental rights of the European Union, Directive 95/46/EC, United Nations Charter, regulation (EC) n° 2271/96 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom, argues that the DI lacks the jurisdiction to make these kind of orders.
48 N° T 4355-15. The same court also handed down a judgement in Google's favour in a second case FT 8038-16, on 23 December 2016. The complainant was not requesting the dereferencing of links per se but an indemnity from Google for breaches to his privacy which indexing links to a discussion forum had allegedly caused him.
49 The first instance court's judgment was upheld on appeal by the Court of Appeal of Svea (Svea Hovrätt) in a judgement dated 5 March 2017(T4721---7).

THE RIGHT TO BE FORGOTTEN IN SWEDEN

was justified, by, as Google argued, the novelty of this issue in Swedish law and the size of the stakes involved in this trial for Google. These two factors explained the extent of the defendant's investigations and therefore their cost.

The case was as follows: on 20 January 2015, Mr R. H.,[50] the complainant, asked Google's Swedish subsidiary (Google Sweden AB) to remove seven links which appeared in the Google Searches search index. Google refused to remove five of these links arguing that as they contained information concerning the complainant's professional life, they were of interest to the public. Mr H. then applied to the court to order Google Inc and Google Sweden AB to dereference websites on which articles concerning him were published.[51] The complainant who had been the Chairman and Chief Executive of a building company, which had since gone bankrupt, claimed in support of this request that the incriminated articles (three articles published in building magazines in 2010 and 2011, including one with the evocative title "a joker has been excluded from three building sites")[52] contained offensive information and were out of date. He also claimed that the links constituted processing of personal data within the meaning of the 1995 Directive which he had not consented to and that his interests in having his privacy protected overrode Google's or a third party's interest in having the incriminated links endure. In addition to an order for Google to remove the links, the claimant also claimed damages of 10,000 kronor (i.e. 1000 euros) and for his legal costs to be re-funded.

Google submitted that the application should be dismissed because Google's Swedish subsidiary could not be considered to be responsible for the processing, since it had no control over it.[53] The search engine's American operator also disputed the fact that displaying the incriminated links in Google Search violated the Personal Data Act.[54] The operator said that, in any event, the interests of the controller or third parties to whom the data was made accessible, overrode the complainant's interest in having his privacy protected against infringements. Google also used a third argument, saying that Swedish law did not permit the courts to order search engine operators to stop referencing websites because it was not stated by the Personal Data Act.

Two questions, which are relevant for the main aspect of this study on how the Swedish courts help protect individuals against referencing by search engines, emerge from the analysis of the judgement: the circumstantial question on how the interests in issue are weighed out and of the lawfulness of the incriminated processing (A) and the more general procedural question of the court's jurisdiction to order search engine operators to de-index links which potentially infringe privacy (B).

A-Weighing up the interests in issue and the question of the lawfulness of the processing

The Swedish court drew on sources from Swedish law (the Personal Data Act and a judgment of the Swedish Supreme Court), the law of the European Union (the European Charter on Fundamental Rights, the ECJ's case law and the guidelines of the Article 29 Data Working Party),[55] as well as the law of the European Convention on Human Rights (the ECHR itself and the case law of the Court in Strasbourg).

The court began its considerations by establishing that the complainant had not consented to the processing which is required by Article 10 of the Swedish Personal Data Act. It then had to decide whether the processing was lawful under point f) of this same provision, which states that processing can occur if it is necessary *"to perform the legitimate interests of the controller or of a third party to whom the data are communicated, if this interest outweighs protecting the privacy of the data subject"*. This requires the court to weigh the complainant's interest in having his privacy and personal data protected against Google's interest in having the search results displayed in the search index and the public's interest in having access to

50 The complainant's name is written as it must be, in full in the judgements. I have decided to only use the complainant's initials.
51 Mr. R. H. appears not to have contacted the DI before he seized the court.
52 The magazines in question are Byggnadsarbetaren (Construction Worker) and Byggvärlden (Construction World).
53 Nor the possibility of taking down the Google search links which are managed by Google Inc.
54 Google deals at length with the balance of interests which it says the judge must carry out. From the point of view of the data subject, this involves the right to privacy and the right to the protection of personal data. Opposite, there is the right of net users to have access to the information as well as Google's right to the freedom of expression and the freedom of trade. This freedom seems to be closely connected (and conditioned by) Google's interest in disseminating information and being perceived as being a reliable search engine from which reliable information is accessible. Google also mentions the interest to publishers in having their information searched on the Internet as well as the interests of the press (reviews periodicals) in publishing the information.
55 Guidelines on the Implementation of the Court of Justice of the European Union Judgment on *Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*", C- 131/12,14/EN,WP 225.

this information whilst making a search using the complainant's name.

The Court took points 81 and 97 of the *Costeja* judgment as the starting point for its assessment, where it is stated that in principle the data subject's fundamental rights under Articles 7 and 8 of the Charter override the economic interest of the operator of the search engine and the interest of the general public in finding the referenced information, yet this is not always the case. Indeed, there can be special reasons, such as the public role played by the person, which justify interfering in this person's fundamental rights because of the public's overriding public interest to have access to the information in question, through its inclusion in the list of results.

After stressing that a person's right to have his or her privacy and personal data protected must be respected, the court[56] then underlined the crucial nature of the freedom of expression (which includes the right to receive and to disseminate information) as a fundamental pillar of democracy.[57] Emphasising the importance of the public's confidence in the reliability of the search results supplied by Google Search or any other search engine, the Swedish court then put more focus on the nature of the complainant's public figure. This was the main criterion which the Swedish court used in the rest of its reasoning, the *special reason* within the meaning of the *Costeja* case law which justifies Google's referencing of the incriminated links.

The Court deduced the complainant's capacity as a public figure, because it was established that he was the CEO of the construction company, which was cited in the incriminated articles when they were published. It also considered this capacity because the complainant had continued to be actively involved in business, as he is also the owner of a company. The court stressed that although the claimant had ceased his activities in the building sector, this had no impact on its assessment.[58]

However, although there is no doubt that M. H. has a role in public life as a businessman, it seems debatable to immediately assert[59] that the complainant is a public figure. This concept, which is more limited than the concept that he has a role in public life, and which it therefore is a "subgroup" of, normally applies to "individuals who, due to their functions/commitments, have a degree of media exposure" according to the Guidelines of the Article 29 Data Working Party. These guidelines also refer to the definition in Resolution 1165 (1998) the Parliamentary assembly of the Council of Europe on the right to privacy, which states "Public figures are persons holding public office and/or using public resources and, more broadly speaking, all those who play a role in public life, whether in politics, the economy, the arts, the social sphere, sport or in any other domain".

In any event, the court would have been better off avoiding opening itself up to criticism on such a crucial part of its reasoning by simply referring to the complainant playing a role in public life, as this would have been sufficient with regards to the weighing up required under points 87 and 91 of the Costeja judgment.[60]

At the very least, it would have been desirable for the court to have, on this precise point, referred to the definitions of a public figure and involvement in public life in the guidelines of the Article 29 Data Working Party.[61]

The Court also examined the *nature* of the incriminated information and the *context* in which it was published. It considered two types of information separately: firstly, information which connects the complainant to the incriminated companies and secondly, information concerning the complainant's alleged dealings with a criminal organisation. Concerning the first information, the court found that this information did not relate to privacy or to the complainant's family life. The judge also noted that the information concerning the complainant's function as CEO of the incriminated companies and their bankruptcy is indisputable and correct and is therefore an argument for considering that the processing is lawful. By so doing, the judge, although referring to the allegations of fraud, omitted to pronounce on their truthfulness although Google had, on this point and the others, carried out detailed searches on all the aspects of M.H's dereferencing demand, and had referred to the size of the complainant's outstanding debts, and the tax issues overshadowing this in its arguments.

The Swedish court begins its assessment of the information on the complainant's alleged connections with a criminal organisation by acknowledging that such information could harm the complainant's reputation. However, it cites the case law on the freedom of

56 P. 18-19
57 In the enacting part of the judgment.
58 P.19.
59 Unless one considers that the publication of the articles themselves gave the complainant the capacity of a public figure which is circular logic.
60 See supra.
61 It should be noted that Google sometimes refers to the complainant's capacity as a public figure and sometimes to his role in public life.

THE RIGHT TO BE FORGOTTEN IN SWEDEN

expression of the European Court of Human Rights[62] to argue that the claimant's privacy has not been violated. In fact, the Swedish court refers to judgments where the court in Strasbourg considered that the publication of information whose veracity had not been confirmed, was not a breach of Article 8 of the ECHR if the data subject had been given the chance of commenting on the information in question.

The Swedish court established in this case that the press article which had been criticised by the complainant clearly mentioned that it was impossible to establish that he had had contacts with the criminal organisation in question and that it was also impossible to prove that threats made against City Hall employees were connected to the complainant. The court also found that the complainant had been given the chance of answering the allegations in the press article and of denying them.

The court also stressed, as a factor which had to be taken into account, that the incriminated information had been published with a journalistic purpose in a review which was dedicated to investigative journalism, and which Google had provided evidence of.[63]

Given the context of the publication, the court found that the information the complainant complained about could be of significant interest to the public especially as it was fairly recent information[64] and concerned a person who was still active in the world of business.

The Court concluded that it resulted from the balance of interests in the case that the interests of Google and the third parties to be able to disseminate and have access to the information contained in the incriminated press articles overrode the complainant's right to the protection of his privacy and his personal data. Consequently, Google's inclusion of links in its search results which were incriminated by the complainant did not constitute an unlawful processing of personal data. Having reached this conclusion, the court said that there was no need to consider whether the court had the jurisdiction to pronounce an order to end the referencing. However, this procedural issue which had been disputed by the defendant (Google) is of interest to us because it is crucial for assessing the extent of the protection which people affected by referencing receive from national courts and beyond this, for assessing the effectiveness of the Swedish protective mechanisms with regards to the requirements laid down by European Union law.

B-The issue of the dereferencing order by the Swedish court

As stated above, Mr R.H had asked the court to order Google to dereference sites with the disputed information. He argued that as it was the controller, it was obliged under the Personal Data Act, *"to take the necessary measures in order to correct, block or destroy the personal data which are incorrect or incomplete with regards to the purposes of the processing"*. He also stated, referring to the *Costeja* judgment, that the controller can be ordered to take such measures if they have not been set up voluntarily.[65]The complainant also claimed that in accordance with the preparatory works (concerning the transposition of the 1995 Directive into Swedish law) *"an individual has a right to bring an action before the court or the Datainspektion, for another individual to be ordered to remove links* (sic!).[66] However, the Internet search engine operator disputed the request for an order by arguing that there was no legal basis for such a power. Google said that this right for an order only existed for a breach of contractual obligations, or if it was stipulated by legislation, which is not the case here, as this power had not been inserted into the Personal Data Act. Google rejected the complainant's interpretation of the preparatory works, considering that they refer exclusively to the Datainspektion's power to pronounce a prohibiting order, subject to a fine.[67]

In his reply, the complainant points out, without developing the argument further, that *"a private person cannot count on the Datainspektion taking his*

62 Notably the judgment of *White v. Sweden*.
63 Google prepared its defence by making searches in reviews in which the incriminated articles had been published, and about the journalist who had written some of them. As the journalist was a reputed journalist who had been nominated for a number of awards, Google concluded that the articles had been published in a serious journal.
64 Here the Court compared the 5-6 years which have passed since publication in this case and the 16 years in the *Costeja* case.
65 Point 77:"Where the controller does not grant the request, the data subject may bring the matter before the supervisory authority or the judicial authority so that it carries out the necessary checks and orders the controller to take specific measures accordingly."
66 P.6.
67 The controversial passage in the preparatory works is as follows: "if there is a disagreement between the controller and the data subject on whether the data should be corrected or not, the data subject can refer the matter to the Data Protection Authority which can pronounce an Order subject to a fine if the law is not respected and ask [the court] to destroy the data or to bring a legal action concerning this before the court". The complainant interpreted this phrase as giving the data subject the right to bring an action before court for an Order, while the defendant considers that the passage in the preparatory works which Mr H refers to only concerns the jurisdiction of the Datainspektion to pronounce a prohibition subject to a fine". 1997/98:44 Personuppgiftslag, p.132.

case on his behalf because it decides which cases it handles itself", and *"for this reason a private person must be able to bring an action before the court"*.[68]

Besides the legal arguments of a purely national nature which I do not take a position on,[69] one might consider that the arguments concerning the effectiveness of the implementation of European law could be emphasised. If the Datainspektion is under no obligation to follow up a complaint and to use its authority to order processing to stop, and furthermore, the courts lack the authority to make such an order, where does this leave the obligation which Member States have under the 1995 Directive to guarantee *"every data subject the right to obtain from the controller [...] the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive"*?[70] Similarly, and above all, where does this leave the implementation of the *Costeja* judgment? Is it sufficient for a court to be able to award compensation for the violation of privacy caused by breach of the Personal Data Act?[71] This is doubtful especially in the context of the indexation of data which, without dereferencing measures, can continue to circulate worldwide *ad vitam aeternam* causing the infringements of privacy which dereferencing is intended to prevent.

Besides the arguments based on effectiveness of the application of European legislation and case law for protecting personal data, one could also refer to the arguments relating to the right to an effective appeal. Thus, the gaps existing in current Swedish law can be highlighted by referring to the Maximilian Schrems C-362/14[72] judgment in which the ECJ said:

> "[...] not providing for any possibility for an individual to pursue legal remedies in order to obtain the rectification or erasure of [such] data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter".[73]

The question is simply asked here.[74]

IV-CONCLUSION

The implementation of the right to be forgotten by the Swedish authorities is still in its infancy. The number of complaints which the Datainspektion has examined concerning refusals by search engines to carry out dereferencing is small, as is the number of cases which have come before the courts. The question has not yet been tackled by an administrative court.[75] However, the entry into force of the General Regulation on Data Protection[76] will no doubt change the situation and also resolve the potential procedural dead-end mentioned above. Those people affected by processing will be given a real right to introduce a claim to the national Data Protection Authority (Article 77), a right which does not expressly exist under the 1998 Swedish Personal Data Act. This right amongst other things, corresponds to the obligation for data protection authorities to process claims[77] and to inform the claimant of the advancement and the outcome of the investigation within a reasonable time (Article 57.1.f). The implementation of these provisions will no doubt result in more frequent examinations by the Datainspektion of claims by people which have been rejected by search engines,[78] which should in turn lead to an increase in the number of appeals by these search engines to the administrative courts. In the face of the probable intensification of the implementation of the digital right to be forgotten by Swedish courts, and with the DI on the front line, it is important that the Swedish state increases the human and financial resources which are allocated to the national Data Protection Authority.

68 P.12.
69 The doctrine is not a great deal of help regarding the court's powers to make orders which explains that the data subject has the right to refer to the judge to "demand compensation for instance". Sören Öman, Hans-Olof Lindblom, Personuppgiftslagen – En kommentar. Norstedts Gula Bibliotek, 1998, 151.
70 According to article 12 of the Directive.
71 Article 48 of the Personal Data Act.
72 *Maximillian Schrems vs Data Protection Commissioner*, 6 October 2015.
73 Point 95.
74 On the question of the European Charter of fundamental rights notably see EU- stadgan- Om grundläggande rättigheter, Carl Lebeck, Studentlitteratur. On the question of the Schrems judgement see Nationella dataskyddsmyndigheter som lagprövare av EU-rätten – en analys av EU- domstolens dom i mål C-362/14, Schrems (Safe harbor-målet), Jane Reichel, Förvaltningsrättsligtidskrift, 2016. On the question of the effectiveness of the law the European union notably see "L'effectivité du droit de l'Union européenne, une exigence renforçant les pouvoirs du juge national", GabrielaAdriana Rusu.
75 This will soon be the case however because Google has appealed the decision of 2 May 2017.
76 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
77 Article 57.1.f.
78 Especially as the obligation by data protection authorities is governed by the right of the data subjects to have "an effective judicial remedy where the supervisory authority [...] does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint [...] (Article 78.2 of the Data Protection Regulation).

UNLIKELY TO BE FORGOTTEN: ASSESSING THE IMPLEMENTATION OF GOOGLE SPAIN IN THE UK THREE YEARS ON

By David Erdos
University Senior Lecturer in Law and the Open Society and Deputy Director of the Centre for Intellectual Property and Information Law (CIPIL) at the Faculty of Law, University of Cambridge

Despite both *Google Spain's* controversial nature and the generally reticent approach of the UK to European data protection, evidence suggests that this judgment has fallen on fairly fertile ground in this jurisdiction. The uptake of newly recognised 'right to be forgotten' rights has been relatively strong, the UK Information Commissioner's Office (ICO) has activity engaged in this area and the UK courts have even reacted sympathetically to wider claims made by some data subjects. Undoubtedly, many issues remain to be resolved. Nevertheless, evidence so far suggests that, even as the UK-EU relationship changes, the essence of the *Google Spain* judgment will survive in the UK.

In finding that search engines had positive data protection obligations arising from their indexing of public domain personal data, the *Google Spain* right to be forgotten ruling in May 2014 quickly came to symbolize the breadth and ambition of EU data protection.[1] Given that the UK has often been rather critical of these characteristics of EU law in this area, it might be expected that this Court of Justice judgment would be implemented here in a distinctly lacklustre fashion. In many respects, however, this does not seem to have been the case. It is true that there was some initial political backlash, with the House of Lords EU Committee questioning whether a search engine should be classed as a data controller and arguing that it was not "reasonable or even possible for the right to privacy to allow data subjects a right to remove links to data which are accurate and lawfully available".[2] The Information Commissioner's Office (ICO)[3] (the UK's Data Protection Authority (DPA)) has also adopted a more pragmatic formulation of the judgment's terms than that suggested by the pan-EU Article 29 Working Party.[4] At the same time, however, the ICO has remained very much actively engaged in the area. Even more strikingly the (albeit only interim) case law from UK courts has positively explored the notion than search engines have wider responsibilities here beyond simply deindexing particular URLs from a name search after specific notice that the processing violates data protection norms. Finally, the uptake of right to be forgotten rights in the UK after this judgment has been comparatively extensive compared to most other major EU jurisdictions.

I-UK IMPLEMENTATION OF GOOGLE SPAIN BY GOOGLE (AND OTHER SEARCH ENGINES)

Although as legal scholars we naturally gravitate towards analysing court and regulatory decision-making, it is important to recognise that the vast majority of right to be forgotten claims lodged against search engines end at the point of being assessed by these actors acting as the data controller. Moreover (perhaps unsurprisingly given its over 90% market share of search in Europe)[5] only one actor is generally involved, namely, Google. By May 2017, Google had received[6] approximately 725,000 claims asserting a right to be forgotten relating to over 2 million distinct URLs.[7] Within this overarching

1 Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014]
2 European Union Comittee, *EU Data Protection Law: A 'Right to be Forgotten'?* (HL 2014-15, 40-I) para 61
3 Information Commissioner's Office, 'Home' <https://ico.org.uk/>
4 European Comission, 'Article 29 Working Party' (22 November 2016) <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083>
5 Matt Rosoff, 'Here's How Dominant Google Is In Europe' (Business Insider UK, 29 November 2014) <http://uk.businessinsider.com/heres-how-dominant-google-is-in-europe-2014-11?r=US&IR=T>
6 Google, 'Search Removals under European Privacy Law' (Transparency Report) <https://transparencyreport.google.com/eu-privacy/overview>
7 In contrast, the next most popular search engine Microsoft Bing

THE RIGHT TO BE FORGOTTEN IN THE UK

figure, some 108,000 claims have been lodged in the UK relating to around 265,000 URLs. This suggests a relatively strong up-take of this newly validated right from UK citizens/residents. In comparison, in Spain itself only around 59,000 claims have been made regarding some 174,000 URLs. Indeed, amongst the large EU jurisdictions, only French citizens/residents seem to have exhibited more interest in these new possibilities, having made some 230,000 requests so far relating to around 420,000 URLs. Google has disclosed an overall breakdown indicating that it has rejected approximately 57% of URLs requests and accepted 43% of these across the EEA (as regards UK-based claims these figures are 61% and 39% respectively). In general, however, it has been relatively opaque about how it assesses claims. Its FAQ on the subject[8] suggests that it only acts on specified URL links following *ex post* demands from individuals with European citizenship and/or residence[9] and only deindexes against searches made under their name and generally only in relation to European-badged search services (although in a change from initial practice (pp. 3-4)[10] it does now indicate that it also deploys (imperfect) geolocation technology to extend this to any search service accessed within the country in which claim is lodged including on e.g. *google.com*). Substantively, it also appears to have narrowly construed *Google Spain* as granting rights only over personal information which is "inadequate, irrelevant, no longer relevant, or excessive" rather than that which violates other requirements of the European data protection, such as accuracy. Finally, it indicates that it notifies original Webmasters of redactions (although elsewhere it has stated that from early 2015 it has now stopped doing so in relation to redactions from malicious porn sites (p. 29)).[11]

II-UK IMPLEMENTATION OF GOOGLE SPAIN BY THE INFORMATION COMMISSIONER'S OFFICE

If data subjects are dissatisfied with the search engines' approach, then their most obvious next port of call is their local DPA. EU DPAs collectively responded to *Google Spain* through a set of Guidelines[12] issued by the Article 29 Working Party[13] in November 2014. Probably partly reflecting DPAs' very limited resources, these Guidelines only took issue with a narrow range of the limitations, which Google (and indeed other search engines) had read into the judgment. Firstly, they suggested that to ensure "*effective and complete protection*" of data subjects, de-listing must be "*effective on all relevant domains, including .com*" (p. 9). Secondly, they argued that routine communication "*to original webmasters that resulting relating to their content had been delisted*" was simply illegal and that even if prior contact with these publishers was in principle legitimate in particularly difficult cases it was then vital that it "*take all necessary measures to properly safeguard the rights of the affected data subject*" (p. 10). Third and finally, rather than focusing only on the substantive elements at play in the *Google Spain* case itself, the Working Party indicated that the data subject could point to any breach of the "*data protection principles*" (p. 11), specifically flagging up issues additional to those in play in the *Google Spain* case, notably data accuracy.

Turning directly to the approach and role of the UK's ICO, shortly after the issuing of the pan-EU Guidelines above, the ICO issued delisting criteria,[14] which closely matched that developed by the Working Party. It also indicated – especially through the development of a *sui generis* online form[15] – that it was open to data subject's addressing concerns to it regarding a search engines' refusal to deindex material against a name search. Since this time, the ICO appears to have analysed approximately 800 such claims including over 120 in

disclosed that up to December 2016 it had received only around 18, 000 claims relating to around 50,000 URLs.

8 Google, 'European Privacy Requests Search Removals FAQs' (Transparency Report Help Center) <https://support.google.com/transparencyreport/answer/7347822/?hl=en>

9 Or, perhaps, a cognate connection to a European country.

10 Peter Fleischer, Global Privacy Counsel, Google, 'Letter to Isabelle Falque-Pierrotin, Chair, Article 29 Working Party' <https://docs.google.com/file/d/0B8syaai6SSfiT0EwRUFyOENqR3M/preview>

11 University of Cambridge, Faculty of Law, Centre for European Legal Studies, 'EU Internet Regulation After Google Spain: Report of Proceedings' (27 March 2015) <https://www.cels.law.cam.ac.uk/sites/www.law.cam.ac.uk/files/images/www.cels.law.cam.ac.uk/documents/google_spain_conference_report_-_16.12.2015.pdf>

12 Article 29 Data Protection Working Party, 'Guidelines on the Implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc v. Agencia Española de Protección de Datos(AEPD) and Mario Costeja González' C-131/12 (14/EN AP225, 26 November 2014) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf >

13 European Commission, 'Article 29 Working Party' (22 November 2016) <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083>

14 Information Commissioner's Office, 'Search Result Delisting Criteria' <https://ico.org.uk/for-organisations/search-result-delisting-criteria/>

15 Information Commissioner's Office, 'Internet Search Results' <https://ico.org.uk/concerns/search-results/>

THE RIGHT TO BE FORGOTTEN IN THE UK

2014/5[16] (p. 34), over 370 in 2015/16[17] (p. 24) and 300 in 2016/17.[18] Whilst not insignificant, this only represents perhaps 1-1.5% of claims for deindexing which have been rejected by Google (and other search engines). In his overview of the first year and a half of *Google Spain* implementation,[19] the then UK Deputy Information Commissioner David Smith indicated that ICO had rejected 40% of concerns on grounds of material or jurisdictional scope,[20] had upheld the search engines' decision in a further 40% but indicated that further action was required in the remaining 20%. Meanwhile, in its 2015/16 and 2016/17 figures, the ICO has indicated that it has found need for more delisting in one third of cases.

Whilst being relatively explicit as regards substantive delisting criteria, the ICO's formal guidance has avoided confronting even the other tricky aspects of the judgment, which were highlighted by the Working Party, namely, the appropriate territorial reach of deindexing and the legitimacy or otherwise of Webmaster notification. Nevertheless, both issues were at least tangentially addressed in the only case so far which has resulted in the ICO using its criminally-backed Enforcement Notice powers. In sum, in this complex and rather troubling case from the summer of 2015, Google had previously removed some links to an old newspaper story online concerning a minor criminal offence committed almost ten years previously. However, after being tipped off through Google's Webmaster notification, the newspaper and then others wrote stories about this,[21] in the process repeating details of the original conviction. These stories were not only widely publicised but, worst still, were readily available through a name search on Google. However, despite a new exercise of the right to be forgotten, Google refused to ensure deindexing arguing that the stories were relevant and in the public interest. Without addressing itself to the legitimacy of Webmaster notification (or to the fact that a substantial portion of the UK media was using this data to republish deindexed stories),[22] the ICO held that Google was obliged to deindex the new stories which included details of the old conviction. This Enforcement Notice was initially formally ambiguous as to its territorial reach. However, the ICO subsequently issued a clarified Notice making clear that it required that Google ensure that the relevant links were not visible to anyone directly accessing any Google search services from within the UK.[23] Although Google appealed the Notice at first, it ultimately agreed to comply (p. 22). [24] This switch was linked to a wider change of policy in early 2016 involving the generic use of geolocation technology as noted above.[25] Thus, although the ICO's actions here are far less severe than the French DPA's decision requiring truly globally effective deindexing[26] or the Spanish DPA direct enforcement against Google's Webmaster notification practices,[27] the UK ICO cannot be said to have entirely ignored the two background issues arising here.

III-UK IMPLEMENTATION OF GOOGLE SPAIN BY THE COURTS

In the main, however, appeal to the ICO has only proved

16 Information Commissioner's Office, *Information Commissioner's Annual Report and Financial Statements 2014/15* (HC 2014-15, 98-I)
17 Information Commissioner's Office, *Information Commissioner's Annual Report and Financial Statements 2015/16* (HC 2015-16, 212-I)
18 Information Commissioner's Office, 'Data protection Reports and Concerns 2016/17' <https://ico.org.uk/about-the-ico/our-information/annual-operational-reports-201617/data-protection-reports-and-concerns/>
19 D Smith, 'Has the Search Result Ruling Stopped the Internet Working?' (Information Commissioner's Office, 2 November 2015) <https://iconewsblog.org.uk/2015/11/02/has-the-search-result-ruling-stopped-the-internet-working/>
20 Which, given especially the case law noted below, are probably sometimes at least highly debatable.
21 C Thom, 'Google 'Right to be Forgotten' Dispute with Information Commissioner will Impact News Archives' (PressGazette, 10 September 2015) <http://www.pressgazette.co.uk/google-right-to-be-forgotten-dispute-with-information-commissioner-will-impact-news-archives/>
22 J Powles, 'Why the BBC Is Wrong to Republish 'Right to be Forgotten' Links' (The Guardian, 1 July 2015) <https://www.theguardian.com/technology/2015/jul/01/bbc-wrong-right-to-be-forgotten>
23 Information Commissioner's Office, 'ICO Orders Removal of Google Search Results' (News, 20 August 2015) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/08/ico-orders-removal-of-google-search-results/>
24 Information Commissioner's Office, *Information Commissioner's Annual Report and Financial Statements 2015/16* (HC 2015-16, 212-I)
25 F Lardinois, 'Google Now Uses Geolocation to Hide 'Right to be Forgotten' Links from its Search Results' (TechCrunch, 4 March 2016) <https://techcrunch.com/2016/03/04/google-now-uses-geolocation-to-hide-right-to-be-forgotten-links-from-its-search-results/>
26 CNIL, 'Droit au Déréférencement : La Formation Restreinte de la CNIL Prononce une Sanction de 100.000 € à L'Encontre de Google' (24 March 2016) <https://www.cnil.fr/fr/droit-au-dereferencement-la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-100000-eu>
27 D Erdos, 'Communicating Responsibilities: The Spanish DPA targets Google's Notification Practices when Delisting Personal Information' (The International Forum for Responsible Media Blog) <https://inforrm.org/2017/03/21/communicating-responsibilities-the-spanish-dpa-targets-googles-notification-practices-when-delisting-personal-information-david-erdos/>

a positive way forward for (some) data subjects seeking a narrow deindexing remedy i.e. the redaction of pre-specified URLs against a name search using European-focused services and only after having given the search engine a good period of time to respond. In contrast, court action has resulted in a couple of data subjects with the resources to engage in this arena securing rather wider remedies. Moreover, despite both cases settling prior to final judgment, it has also resulted in judicial *dicta* which appears receptive to the possibility that such wider remedies may be legally mandated at least in certain circumstances. In the first case, Daniel Hegglin, a Hong Kong businessman and Swiss national with business and personal links to the UK[28] was confronted with a large number of abusive and defamatory allegations online accusing him, for example, of being a "murderer, a Nazi, a Klu Klux Klan sympathiser, a paedophile" (at [2]).[29] He sought to require Google to take proactive steps "to ensure that such material does not appear as snippets in Google search results" (at [7]). Notwithstanding that Hegglin was not a British national or resident and that he clearly sought a remedy going considerably beyond simply removing specific URLs on name searches carried out on google.co.uk, on 31 July 2014 Mr Justice Bean granted him leave to serve this claim on Google.com out of jurisdiction (at [22]). The High Court then set aside five days for a full trial in November 2014. However, on the first day of this trial it was announced that the two parties had settled. Whilst unable to disclose the precise details of the agreement, Hegglin's barrister Hugh Tomlinson QC stressed that the case was brought "against Google in order to seek extra assistance to combat a campaign of anonymous and extreme Internet trolling" and that "[t]he settlement includes significant efforts on Google's part to remove abusive material from Google hosted websites and from its search results".[30] In the second case (also argued by Hugh Tomlinson QC), the former head of Formula One Max Mosley sought to require that Google proactively block access to images of him engaging in private sexual activity (originally illegally published in the *News of the World* newspaper in 2008) across not only name but all searches. In a January 2015 decision rejecting Google's attempt to strike out this claim,[31] Mr Justice Mitting held that from the point of view of UK data protection law "[t]he claimant's assertion that he has suffered substantial unwarranted distress [from Google's data processing] is plainly capable of belief, and if so, founding the remedy which he seeks" (at [25]). Moreover, even if the e-Commerce Directive's ban on requiring that certain intermediary actors engage in general monitoring of their services applied here,[32] (which was found to be a debatable point), Mitting J held that "[g]iven that it is common ground that existing technology permits Google, without disproportionate effort or expense, to block access to individual images, as it can do with child sexual abuse imagery, the evidence may well satisfy a trial judge that it can be done without impermissible [general] monitoring" (at [55]). Again, however, Google settled the case just before full trial;[33] whilst the details of the agreement were entirely confidential, Max Mosley's solicitor Tanja Irion described him as being "happy" with the outcome.

IV-CONCLUSIONS

Google Spain placed European data protection within clearly controversial territory. Nevertheless, three years on, the indications are that even in the UK this judgment has fallen on fairly fertile ground. There has been a comparatively strong uptake by UK citizens/residents of these newly validated 'right to be forgotten' rights, with claims for the deindexing of hundreds of thousands of URLs being lodged principally against Google. Meanwhile, the UK's ICO has been fairly actively engaged in this area. Although the number of individual concerns which it has dealt with remains small, it has found that further nominative deindexing has been required in approximately one third of its cases. Meanwhile, whilst considerably more pragmatic than pan-EU Working Party guidance in this area, the ICO's one formal Enforcement Notice mandated that Google use geolocation technology to restrict relevant results in the UK and also addressed some of the troubling consequences of Google's practice of Webmaster notification by requiring a new deindexing of the stories written off the back of the information which Google disclosed. Finally, and perhaps most strikingly,

28 K Rahman, 'Google Settle Court Case with Businessman Who Was Victim of 'Extreme Internet Trolling' After Agreeing to Remove Abusive Material from Search Results' (Daily Mail, 24 November 2014) <http://www.dailymail.co.uk/news/article-2847665/Google-settle-court-case-businessman-victim-extreme-internet-trolling.html>

29 *Hegglin v. Person(s) Unknown & Anor* [2014] EWHC 2808 (QB)

30 K Rahman, 'Google Settle Court Case with Businessman Who Was Victim of 'Extreme Internet Trolling' After Agreeing to Remove Abusive Material from Search Results' (Daily Mail, 24 November 2014) <http://www.dailymail.co.uk/news/article-2847665/Google-settle-court-case-businessman-victim-extreme-internet-trolling.html>

31 *Mosley v. Google Inc & Anor* [2015] EWHC 59 (QB)

32 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L178/1

33 Sky News, 'Mosley Settles With Google Over Orgy Photos' (15 May 2015) <http://news.sky.com/story/mosley-settles-with-google-over-orgy-photos-10359446>

THE RIGHT TO BE FORGOTTEN IN THE UK

the UK courts have responded fairly sympathetically to the idea that, at least in certain cases, wider remedies may be legally mandated such as ensuring deindexing in contexts other than a name search and deploying technology to block particularly problematic content on a proactive basis. Undoubtedly future jurisprudence at both UK and EU level will need to carefully address a number of critical issues largely unanalysed in the judgment, notably the balance required in particular cases with freedom of expression. Nevertheless, the evidence presented here suggests that, even if the current EU-UK Brexit negotiations result in Court of Justice jurisprudence no longer being binding in the UK, the essence of the *Google Spain* judgment will survive even in this jurisdiction. This is not a judgment that will simply be forgotten.

Partie 2 : Quelques aspects matériels du droit à l'oubli numérique en Europe
Part 2: Material aspects on the Right to Be Forgotten in Europe

THE RIGHT TO BE FORGOTTEN AS A POSITIVE FORCE FOR FREEDOM OF EXPRESSION

By Paul Bernal
Senior Lecturer in Information Technology, Intellectual Property and Media Law, UEA Law School, University of East Anglia

The right to be forgotten is generally portrayed as a restriction on freedom of speech, but the situation is more complex than this. In some ways the right to be forgotten works in favour of both freedom of speech and access to information – helping both those who wish to have their work accessed and those seeking information. Indeed, as this paper argues, if the right is properly implemented, the benefits to freedom of expression may well outweigh the risks.

In one of the more dramatic reactions to the proposal for the incorporation of a right to be forgotten into the reform of data protection, Jeffrey Rosen said that it "represents the biggest threat to free speech on the Internet in the coming decade."[1] Though somewhat more hyperbolic a reaction than others, it was not unrepresentative of a strong stream of argument, particularly in the United States. The right to be forgotten was – and often still is – seen as fundamentally in conflict with freedom of expression, a law that acts primarily as censorship, and a way for people to hide their past or even rewrite history.

When, in 2014, the Court of Justice of the European Union (CJEU) ruled that, in one particular way, such a right already existed under the old data protection regime, in the *Google Spain* case[2], the reactions were in some ways even more dramatic. More than 150 academic pieces were written about the subject in the months that followed,[3] many of which noted the conflict with freedom of expression and saw the ruling as fundamentally flawed.[4] Those defending both the right and the decision in *Google Spain* largely defended it in relation to protecting privacy, making Google more accountable, and providing some kind of a check on the dangers associated with the seemingly eternal memory of the internet.

Those arguments have continued ever since the ruling, without reaching any firm conclusion, and have lost their impetus and fire not because of any real resolution but because the right, as implemented by Google (in a way that will be described later in this working paper) has not had as dramatic an effect as the likes of Rosen might have suggested. They are likely to be invigorated by the coming into force of the General Data Protection Regulation (GDPR) in May 2018, when the new version of the right – now described as the right to erasure, with the 'right to be forgotten' only in parentheses – comes into effect.

This working paper, however, is not intended to repeat those arguments. It is not about the way that the right works in relation to privacy, or indeed in relation to the checking or boosting of Google's power. Instead it makes a bolder claim – that rather than being in conflict with freedom of expression, the right to be forgotten, specifically as it relates to search engines as explored in the *Google Spain* ruling, if properly constituted and applied is primarily a positive force for

1. In 2012, in the Stanford Law Review online, at https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/
2. CJEU *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12, ECLI:EU:C:2014:317
3. See Powles and Larsen's compilation of academic commentaries, online at http://www.cambridge-code.org/googlespain.html
4. For example Lyons in TechPolicyDaily (at http://www.techpolicydaily.com/technology/right-forgotten-forget/), Proops for The Lawyer (at https://www.thelawyer.com/issues/online-may-2014/privacy-but-at-what-price/) and academically Kulk, Stefan and Zuiderveen Borgesius, Frederik J., 2014 Google Spain v. González: Did the Court Forget About Freedom of Expression? (September 4, 2014). European Journal of Risk Regulation. Available at SSRN: http://ssrn.com/abstract=2491486

THE RIGHT TO BE FORGOTTEN AS A POSITIVE FORCE FOR FREEDOM OF EXPRESSION

freedom of expression. It generally helps both freedom of expression and its complementary right, access to information, more than it hinders or harms them.

The argument is made through an examination of how search engines work, how search engines are used, and the respective rights of different parties involved – some of whose rights have not, at least in general, been considered in the debate at all. Specifically, the right to freedom of expression of those whose stories about a person are not subjected to the right to be forgotten, and the right to access to information of people wanting to find accurate, up-to-date and relevant information about a person. It is the latter, perhaps, that are the most important in the grand scheme of things, particularly when one of the key roles of the internet is considered: its role as a digital reference system.

I-THE ROLE OF INTERNET AS A DIGITAL REFERENCE SYSTEM

The internet has many different roles in today's society. It is a communications medium, a business platform, a political platform, a space for technological innovation and experimentation, a governmental infrastructure and much more. One of the key roles, however, is as a digital reference system. That is, as a system through which information can be accessed, facts can be checked and cross-checked and so forth. The general presumption is that if information is anywhere, it is on the internet. There is a paradox about the nature of this digital reference system: at one level people know that nothing on the internet can be trusted, but on another level they know that they can use the internet to check up on things.

On a practical level, however, the key point is that people use the internet in this way. In particular, people use Google (and to a lesser extent other search engines, because Google still has the lion's share of the search engine market, particularly in Europe) in this way. If you want to find out information, you 'Google' it. If you want to check information about a particular person, you Google it. This may not be the only thing that you do to find the information or test some other information that you have obtained in some other way – but it is likely to be one of the main things that you do, particularly if the matter is not of the highest importance. In general practice, by the general population, it can reasonably be seen as something 'normal' to do.

This means that there is a public interest in the way that the internet functions, the way that search engines function – and specifically in the way that Google functions. If people are to use the internet as a digital reference system, and use Google as the means to access it – and the route to the information – they have an interest in that reference system being reasonably accurate and up-to-date, and in that means of access presenting them with the most appropriate (and again accurate and up-to-date) information.

II-A PUBLIC INTEREST IN SEARCH MECHANISMS?

How, then, is that public interest – in effect the right of the public to access to information – to be satisfied? Without such mechanisms as the right to be forgotten, it is in essence relying on the appropriate functioning of the Google algorithm. When something is searched for, it is that algorithm that determines what is presented, and in what order. This latter part, the order in which search results are presented, has been noticeable by its absence in many of the analyses of the effects of the right to be forgotten, and yet in practical terms it may be the most important part of the process. In 2009, Van Deursen and van Dijk's empirical research[5] indicated that more than 90% of people searching do not read beyond the first page of search results, and more than 50% do not read beyond the first three results on that first page. Subsequent research has confirmed the essence of these findings[6] - which has a direct and very significant effect. It is not just whether a link can be found through a search engine that matters in practice, but where that link can be found. Though what might loosely be described as freedom of expression and access to information 'purists' might care only about the 'right' to access – if the information can actually be found, whether on page 1 or page 100 of the search results, then that 'right' is satisfied – the practical result of having information lower down on a search page is that this information, in practice, is never found.

That in turn has two significant implications. Firstly, that the information about a person determined by a search may be incomplete, unbalanced and not up-to-date if important, relevant and up-to-date information is too far down the search results to be found in practice. Secondly, that the speech 'rights' of those who have produced important, relevant and up-to-date information are impacted upon by the placement of links to their pages.

6. Using the Internet: Skill Related Problems in User Online Behavior; van Deursen & van Dijk; 2009, online at http://www.alexandervandeursen.nl/Joomla/index.php/publications/published-articles/30-using-the-internet-skill-related-problems-in-users-online-behavior

This, it can be argued, means that people have a right to have their pages treated fairly and appropriately by Google. Indeed, this is something that has been considered in a related context in the dispute relating to the UK search site Foundem[7] and the ongoing anti-trust investigation into Google Shopping.[8] In those examples, the question was effectively whether Google were either prioritising results that benefited them or 'demoting' results of what were in effect competitors.

That these are issues primarily of competition law rather than anything immediately connected to freedom of speech (though these ar in essence speech rights) should not distract from the relevance here. Indeed, it should emphasis the complexity and paradoxical nature of our relationship with Google: sometimes we treat it as a neutral indexer of the internet, working for our benefit in the service of freedom of speech and access to information, and sometimes as a purely profit-driven mega-corporation with only its own interests at heart. That paradox will be examined further in the conclusion to this paper.

At this stage, however, the key thing to note is that it does matter where results appear on the search page. Indeed, it is arguable that appearing, but outside the first page, has more similarity in effect with not appearing at all than it does with being on the first page. The exclusionary effect of being placed beyond the first few results is in practice the same as being excluded from the rankings entirely.

III-THE RIGHT TO BE FORGOTTEN AND SEARCH RESULTS

This needs to be considered when looking at the impact of the right to be forgotten – or to be more precise the right to be delisted, as set out in the *Google Spain* case. How this works in practice needs to be made clear. The relevant part of the CJEU ruling in *Google Spain* was in effect that an item should be excluded from the results of a search for a particular name. As Google interpreted the ruling, this was where a result was 'inadequate, irrelevant, no longer relevant, or excessive'.[9]

As implemented, that means that certain links would no longer appear if you searched for that particular name: it would be 'delisted'. To understand how this impacts upon search rankings as well as what is simply included within the search results, consider a search for a person whose name is Hypo Thetical. Before the right is applied, imagine that the results for the search are:

1: "Story concerning a very important crime for which Hypo Thetical was one of many victims, but named specifically."

2: "Another version of the story about the very important crime for which Hypo Thetical was one of many victims"

3: "Yet another version of the story about the very important crime for which Hypo Thetical was one of many victims"

4: "Old and irrelevant story about Hypo Thetical"

5: "Relevant and important story about Hypo Thetical

6: "Reasonably interesting story where Hypo Thetical is mentioned"

7: "Interesting and relevant link to work by Hypo Thetical

8: "Another interesting link analysing work by Hypo Thetical by Another Writer

9: "Critical analysis of Hypo Thetical's work by A Sceptic"

Based on the evidence above about how people in practice use search results, without the right to be forgotten being applied, the vast majority of people would only click on the story about the very important crime. A few would click on the old and irrelevant story about Hypo Thetical, and one or two on the relevant and important story. Almost none would find the 'interesting and relevant link' to Hypo Thetical's work, or the link to the analysis of Hypo Thetical's work by a third party.

The detailed ways that search engines work, including their algorithms, are closely guarded trade secrets, and in all probability justifiably so. What we do know is that they use popularity and links as part of the process – a page that is already popular is more likely to be one that is found. This is logical, and does in practice mean that search engines take people to where others in the same situation have gone before, and to sites that have proven their worth, but it can also mean that 'important' and 'newsworthy' information can be prioritised where it should not necessarily be so. In the case of Hypo Thetical it might well mean that the stories which are very important in themselves but not so important in relation to Hypo Thetical, particularly in terms of Hypo Thetical's current life, find their way to the top of the search results. That then dominates the information about Hypo Thetical that is discovered through search.

Consider then applying the right to be forgotten. Hypo

7. See for example Lao, Marina, 'Neutral' Search as a Basis for Antitrust Action? (April 4, 2013). Harvard Journal of Law and Technology Occasional Paper Series -- July 2013. Available at SSRN: https://ssrn.com/abstract=2245295
8. See http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39740
9. https://www.google.co.uk/policies/faq/

THE RIGHT TO BE FORGOTTEN AS A POSITIVE FORCE FOR FREEDOM OF EXPRESSION

Thetical asks for the stories concerning their victimhood in the crime to be delisted, and for the Old and Irrelevant story to be delisted, and Google complies. The first four results are then removed, and the search results read:

1: "Relevant and important story about Hypo Thetical

2: "Reasonably interesting story where Hypo Thetical is mentioned"

3: "Interesting and relevant link to work by Hypo Thetical

4: "Another interesting link analysing work by Hypo Thetical by Another Writer

5: "Critical analysis of Hypo Thetical's work by A Sceptic"

What needs to be noted is that it is not just that the delisted links are removed, but that the links that were below them in the search results have been promoted. From the perspective of most searchers, this is a far more valuable selection of links concerning Hypo Thetical – and it must be remembered that this change applies only for searches directly concerning Hypo Thetical. In terms of access to information, the result after the right to be forgotten is applied are better than they were before it.

IV-THE RIGHT TO BE FORGOTTEN AND FREEDOM OF EXPRESSION

We need to consider whose speech and access to information rights are being impacted upon by this kind of application of the right to be forgotten, and in what way. The negative impact upon freedom of speech has been discussed many times, as noted above, but it is important to be clear about exactly who is affected.

The first 'person' whose rights are impacted upon is Google. Google at times seems to portray itself as a kind of 'mere conduit', organically generating results for which it has little direct responsibility, and at other times as a clear 'speaker' with what in the US are set out as First Amendment rights.[10] The right to be forgotten clearly impacts directly upon Google's freedom of expression, limiting what they can say in their search results. How much it impacts upon their freedom is one of the key factors to be considered when looking at the overall impact of the implementation of the right.

The second set of people whose rights are impacted upon negatively are those whose stories are delisted: the writers of journalistic pieces or blogs, the publishers and others involved. Their pieces of work will not be linked to as much, and will not, therefore, be read as much.

The third set of people whose rights are infringed are those who might want to read those stories, rather than the more apparently relevant stories which have been promoted as a result of the removal of the delisted links.

Next, consider those whose speech and access to information rights are being affected positively by the change brought about by this application of the right to be forgotten. First and most obviously, the searchers who were looking for accurate, relevant and up-to-date information about Hypo Thetical. They have been able to find that information more easily – indeed, they may actually find it rather than pass it by. Their rights have been enabled through the application of the right to be forgotten.

The second group, and the group generally ignored in the analysis of the right to be forgotten, are those whose links have been promoted by the application of the right. In this case, the journalists who wrote the 'relevant and important' story and 'reasonably interesting story' which moved up to the top of the search results will have their stories found and read more often. Hypo Thetical's own speech rights (as opposed to their privacy and reputational rights which have been more often considered in the balancing exercise) have been enhanced by the rise of their work from 7th (and rarely read) to 3rd (and much more commonly read) in the list. Similarly, the rights of Another Writer and A Sceptic have been enabled – their works have gained much more prominence, and might even have moved from the second (almost never read) page of search results to the first.

The situation, therefore, is not as simple as it might seem at first. The right to be forgotten does not just have a negative impact on freedom of expression and access to information, but a complex one, with positive effects on some and negative effects on others. The question then to ask is how to balance those effects, and what the overall impact of the application of the right is upon freedom of expression and access to information.

V-BALANCING RIGHTS?

The first step is to consider what the purpose of freedom of expression is intended to be – and, further,

[10] See for example Volokh, Eugene, and Falk, Donald M, 2012, First Amendment Protection for Search Engine Results, online at http://volokh.com/wp-content/uploads/2012/05/SearchEngineFirstAmendment.pdf

what the purpose of human rights is in general. Barendt described his four 'grounds' for freedom of speech as:

(i) The discovery of truth

(ii) As a necessary element of self-fulfilment

(iii) To enable citizens to participate in democracy

(iv) Suspicion of government[11]

Barendt, it should be noted, was considering freedom of speech for individuals rather than corporations – precisely how the speech rights of Google should be considered, outside of a technical First Amendment discussion is on these terms at least a difficult if not entirely moot point. It should further be noted that, in more general terms, human rights are intended to empower the relatively weak and protect them against the relatively strong. In more traditional terms, this means protecting individuals against the state, but in a more complex environment where corporate power is increasingly important this must also mean protection from the often overwhelming power of the corporations.

That then brings a question of whose speech and information rights are being impinged upon in a more harmful way, and whose are being aided more appropriately by the inclusion of exclusion of the right to be forgotten. Do the rights of those whose stories might no longer be linked to outweigh the rights of those whose stories will as a result get more exposure?

When Barendt's four grounds are considered, the first is the most important in this context. Both sides have a claim to it – but if the terms of the right to be forgotten are applied well (an important caveat that will be discussed below) then the claims of those whose stories are 'inadequate, irrelevant, no longer relevant, or excessive' are unlikely to outweigh those whose stories are not.

When the rights of those seeking information – the discovery of truth, in Barendt's terms – are taken into account, the balance shifts further in the direction of the right to be forgotten as a positive force, again with the crucial caveat of appropriate application being taken into account. Search results with 'bad' results stripped out are better search results, making the discovery of truth easier.

The second ground – the necessary element of self-fulfilment – is harder to assess, though when what might be called the 'reputational' elements of search results from a personal search are taken into account, the rights of the person being searched for are likely to outweigh those whose stories are being excluded from searches for that person. The same might be said of the third ground – the reputational side as well also comes into play – whilst the fourth ground is not directly relevant, or at least should not be, as will be discussed when considering the all-important caveats.

The next question is how Google's freedom of speech rights fit into the equation. Google's role in providing an opportunity for others to express themselves and to seek information has, in effect, already been taken into account when considering the rights of those people. Google's own rights are rather different. They do not really fit into Barendt's terms: a corporation does not have any need to discover truth, or any need for self-fulfilment, nor to participate in democracy or to be suspicious of government. That does not mean that Google has no speech rights – but it does mean that they are somewhat different, and should be weighed somewhat differently in the balance. As an enabler of others' rights, Google is crucial. As a claimant of its own rights, it is hard to argue that Google holds such an exalted position. Indeed, it is more arguable that Google's rights and needs in this area are primarily commercial rather than speech related.[12]

There are two other important considerations to add to the picture. The first is to remember that in its current form, as implemented by Google and as ruled by the CJEU (according to most interpretations) the impact is only on links. Source information, and actual stories are not deleted. Thus the speech rights of those who have written those stories are not restricted as much as they might appear. This isn't rewriting of history, just a minor alteration in the index, and only where it relates to searches using the name of the subject. When the GDPR comes into play and with it the possibility of demanding the deletion of source data, very different balances need to be made. Delisting a story from particular search results is very different in speech terms to demanding its entire deletion from the internet.

The second is to look at the relative power of those involved, remembering that rights are intended to protect the weak from the strong. Part of the reason for this is that the relatively strong generally have other ways to exercise their rights – particularly in comparison to the weak. Here, Google have immense power, so putting a minor restriction on their speech rights (and again, the caveats need to be considered very carefully) should not be considered impossible if by doing so the

11. From Barendt, E, Freedom of Speech (OUP 2005) p7, 13, 18, 21 respectively
12. See Bernal, P.A., 2014, '"The EU, the US and the Right to be Forgotten": Chapter 4 in 'Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges', Springer

speech rights of those weaker than them are improved as a result.

VI-CRUCIAL CAVEATS

As noted a number of times above, all of this is predicated on the right to be forgotten – in its 'delisting' form – being implemented in an appropriate form. It means not allowing it to be used to reduce access to important and relevant information, or to protect powerful people against scrutiny. Theoretically this should be the case: it should not apply to 'public figures', and Google's decisions about whether to accept a delisting should be based on exactly these kinds of criteria.

Whether it actually does so in practice is not as easy to be clear about. The surface level information in Google's transparency report[13] appears reasonable, and the data scraping exercise by Sylvia Tippmann and Julia Powles[14] suggests that the right has generally been used in appropriate ways, removing links to private information on social media sites rather than information important in public terms – but it is hard to be certain. Google's transparency report is very limited, and the examples they provide are self-selected and how representative they are of the underlying trends is impossible to verify.

Without more clarity and transparency on the implementation, the theoretical benefits to freedom of expression outlined above cannot be supported in practice. More transparency is needed. Google has so far resisted this: the letter from 80 academics in the field in May 2015[15] requesting this has not yet be responded to in any meaningful way. If the right to be forgotten is to be something positive, this is critical.

VII-A POSITIVE RIGHT TO BE FORGOTTEN

It should be possible to achieve. The benefit of a well-implemented right to be forgotten could be massive for an individual who uses it, significant for those whose stories are 'promoted', and the harm is unlikely to be significant on those whose stories are demoted or delisted.

There is, however, a bigger point here, one that may be both the best and the worst point about the right to be forgotten in its delisting form. What it does is interfere with the search algorithm – and that kind of interference is sometimes seen as interfering with the essence of the free internet itself. It is not in any way the only such piece of interference: the scale of delisting on the basis of copyright infringement dwarfs that of the right to be forgotten, and continues to rise whilst the right to be forgotten implementation has essentially stabilised, whilst sites that contain other illegal content such as child abuse imagery are appropriately delisted.

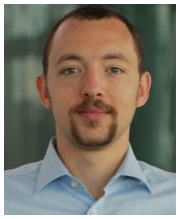
This can be a positive development: search results are generated by algorithms that should not be assumed to be neutral or faultless. They can build in bias and have discriminatory effects: the drive towards algorithmic accountability is growing as a consequence. They can be 'gamed' – there is an entire industry built around 'search engine optimisation', which is essentially about finding ways to manipulate search results. They can polarise and at times damage access to real and important information: the 'fake news' furore that came to the fore in 2016 emphasises this point. The right to be forgotten should be seen in the context of this larger problem and bigger issue.

On the other side of the coin, and perhaps the biggest point against the right to be forgotten is that it could open the doors to the negative side of this kind of manipulation. Allowing governments to control search results directly, or to pressurise search engine operators to do so with the threat of legislation or other sanctions if they do not, could allow the powerful to use this kind of control against the weak, stifling dissent, enforcing harsh blasphemy or indecency rules, restricting access to information about political figures and so forth. That, however, is happening to an extent anyway.

The key to making this work is, as is often the case, to keep monitoring, increase transparency, and be~~ing~~ prepared to look at new ways to do things. If the right to be forgotten seems to be being misused, another approach should be considered. If, as currently appears to be the case, it (at least in general) is not being misused, then those whose objections to it are based on freedom of speech in particular should be prepared to look at the other perspective. The right to be forgotten can have a positive impact on both freedom of expression and access to information. Whether it will or not is something that we need to keep watching.

13. https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en
14. See for example https://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests
15. See for example https://www.theguardian.com/technology/2015/may/14/dear-google-open-letter-from-80-academics-on-right-to-be-forgotten
16. See for example https://techcrunch.com/2016/09/08/the-need-for-algorithmic-accountability/

IMPLEMENTING THE RIGHT TO BE FORGOTTEN: TOWARDS A CO-REGULATORY SOLUTION?



By Nicolo Zingales
Lecturer in Competition and Information Law
School of Law, Politics and Sociology
University of Sussex

By Agnieszka Janczuk-Gorywoda
Assistant Professor in European Economics Law, Utrecht University, Law School

Insufficient attention has been put into the enforcement of the Right To Be Forgotten as a measure of private regulation. In this contribution, we begin sketching a regulatory solution to the above challenges which builds upon the efficiency of private regulators, while at the same time aiming to ensure that these operate within a rule of law framework offering adequate safeguards for the pursuit of the public interest.

In *Google Spain*[1], the CJEU established a so called "right to be forgotten" (RTBF), i.e. for individuals to obtain the erasure from the results of search engines prompted by a search for their name, whenever the information linked in the results is "inadequate, irrelevant or no longer relevant, or excessive".[2] This judgment is revolutionary not only for the far-reaching consequences of the principle it affirms, but also because it leaves in the hands of a private entity (though subject to possible appeals) the responsibility of implementing such principle.

Yet, insufficient attention has been put into the enforcement of the RTBF as a measure of private regulation. Governance studies teach us that private regulators should operate within limits, designed to prevent potential abuses and adequately safeguard the public interest. A vast body of literature defines principles of good governance in the context of private regulatory solutions, such as access, openness, procedural fairness, transparency, participation and effectiveness.[3] A close observance of these principles is crucial when delegation of private law-making triggers extraterritorial effects, as is currently the case under the implementation of the RTBF taken by the French Data Protection Authority (DPA), the Commission Nationale de l'Informatique et des Libertés (CNIL).[4] In this working paper, we begin sketching a regulatory solution to the above challenges, which builds upon the efficiency of private regulators, while at the same time aiming to ensure that these operate within a rule of law framework offering adequate safeguards for the pursuit of the public interest.

I-THREE CONTROVERSIAL ISSUES IN THE IMPLEMENTATION OF THE RTBF

A-Discretion in adjudicating private claims

Despite the revolutionary nature of the obligation imposed on search engines to address individual requests for de-listing, major industry players such as Google, Microsoft Bing and Yahoo! implemented the

1. CJEU *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12, ECLI:EU:C:2014:317
2. Id., para. 94.
3. E.g. DC Esty, 'Good Governance at the Supranational Scale: Globalizing Administrative Law' (2006) 115 Yale Law Journal 1490; D Curtin and L Senden, 'Public Accountability of Transnational Private Regulation: Chimera or Reality?' (2011) 38 Journal of Law and Society 163; C Scott et al., 'The Conceptual and Constitutional Challenge of Transnational Private Regulation' (2011) 38 Journal of Law and Society 1.
4. See a summary of the relevant decisions at https://www.cnil.fr/fr/node/15790 and https://www.cnil.fr/en/right-delisting-google-informal-appeal-rejected-0; See also I Falque Pierrotin, 'Pour un droit au déréférencement mondial', Débats du Monde (29 December 2016), at https://www.cnil.fr/fr/pour-un-droit-au-dereferencement-mondial.

IMPLEMENTING THE RIGHT TO BE FORGOTTEN: TOWARDS A CO-REGULATORY SOLUTION?

ruling quite swiftly[5] , readily making available a web form for users to submit their requests. Despite some commonalities, the forms differ widely in terms of the substantive information they require in submission of a delisting request. For example, while Google and Yahoo provide a blank space in the form for individuals to explain how the page relates to the data subject and why its content is "unlawful, inaccurate, or outdated"[6] Microsoft Bing poses a number of additional questions. Specifically, claimants must indicate (1) whether they (and presumably anyone on behalf of whom the application is made) are public figures; and (2) whether they have or expect to have a role in the local community or more broadly that involves leadership, trust or safety.[7] Furthermore, claimants are asked to qualify the information that Bing is requested to "block" as (a) inaccurate or false; (b) incomplete or inadequate; (c) out-of-date or no longer relevant; or (d) excessive or otherwise inappropriate. They are also invited to indicate why their "privacy interest" should outweigh the public's interest in free expression and the free availability of information. Last, but not least, they are given the opportunity to upload supporting documentation.

Ostensibly, Microsoft Bing's procedures incorporate more safeguards to prevent the submission of imprecise, unfounded or unsubstantiated requests. Perhaps this contributes to the higher success rate of requests submitted to Microsoft Bing (67%) than those submitted to Google (43%). There are several factors however that influence the outcome of requests, and thus in the absence of the publication of more detailed statistics and of the criteria used by each search engine in the adjudication process (as "strongly recommended" by the Article 29 Working Pary (A29WP[8]), that remains a speculation. The discrepancy between web forms illustrates in simple terms a central problem in the implementation of the RTBF: a significant amount of discretion is left in the hands of search engines to determine the contours of the RTBF.[9]

This discretion is problematic when it comes to balancing between conflicting rights at stake. The CJEU only gave some very general guidance as to how this balancing should be carried out, requiring a "fair balance" between the legitimate interests of searchers and the data subject's privacy and data protection rights. More controversially, the CJEU stated that the latter rights "override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name".[10] However- the Court continued- that would not be the case "if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question".

This formulation has been criticized for the insufficient attention given to freedom of expression[12] , in particular in casting the right to access to information merely as an interest, much like the economic interest of the search engine, rather than recognizing it as a constituent part of the fundamental right to freedom of expression protected under article 11 of the Charter of Fundamental Rights. More generally, it is arguable that the court could have recognized the instrumental role of search engines for freedom of expression, including the right to free expression of search engine operators themselves.[13]

5. According to press coverage, Google made its form available in June 2014, and Microsoft in July of the same year. It is less clear when the form first appeared on Yahoo!, although it was reported to be already in place on December 1st, 2014. See S Schechner, 'Google Starts Removing Search Results Under Europe's 'Right to be Forgotten', WSJ (June 26, 2014) at https://www.wsj.com/articles/google-starts-removing-search-results-under-europes-right-to-be-forgotten-1403774023; and A Griffin, 'Microsoft's Bing and Yahoo search engines have started to fulfil the controversial requests', The Independent (December 1st, 2014) http://www.independent.co.uk/life-style/gadgets-and-tech/news/microsoft-and-yahoo-join-google-in-deleting-search-results-under-right-to-be-forgotten-ruling-9896100.html

6. For Google, see https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=1-636297647133257433-1626206613&rd=1; for Yahoo, see goo.gl/3qUdTe.

7. See https://www.bing.com/webmaster/tools/eu-privacy-request.

8. See Guidelines on the implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzales" C-131/12 (hereinafter, A29WP Guidelines).

9. See in this sense also J Powles, "The case that won't be forgotten» (2015) 47 Loyola University of Chicago Law Journal 583, 595.

10. Google Spain, supra n 1, para 97.

11. M Peguera, supra n 21, p. 551. S Kulk, F J Zuiderveen Borgesius. 'Google Spain v. González: Did the Court Forget About Freedom of Expression?', European Journal of Risk Regulation 5 (3) (2014), 389, 595; J Powles, supra n 9, 591; E Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos', 14 Human Rights Law Review 761 (2014), 769; M L Rustad and S Kulevska, 'Reconceptualizing the Right To Be Forgotten To Enable Transatlantic Data Flow', 28 Harvard Journal of Law and Technology 349 (2015), 373-374.

12. N van Eijk, 'Search Engines: Seek and Ye Shall Find? The Position of Search Engines in Law', Iris Plus, 2 (2006) 1, 7

IMPLEMENTING THE RIGHT TO BE FORGOTTEN: TOWARDS A CO-REGULATORY SOLUTION?

The A29WP guidelines tried to adjust the mark by recognizing the importance of the freedom of expression of users and original publishers at stake, and offering to DPAs a list of common criteria for handling complaints, which by implication should inform the way in which decisions are made by search engines in the first place. However well crafted, those criteria are far from exhaustive, as they fail to guide complex appreciations of balancing conflicting factors or interests. They thus leave search engines with a number of delicate choices having a substantial impact on the fundamental rights of individuals. This is perceived as problematic for the basic reason that search engines are not public courts, hence employees tasked with making these determinations will not have the same competence and standards of professional ethics and independence that bind members of the judiciary.[14] Relatedly, as private entities are conferred adjudicative power and wide discretion, the nature and depth of balancing may be affected by the economic incentives and the interest of those entities to conduct their business. For example, it is clear that a very probing inquiry into the circumstances of each case would impose serious costs on the search engine; similarly, it runs against the incentives of search engines operators to publish a detailed list of criteria for decisions, as that would make RTBF claims more sophisticated and more complex to decide.

These efficiency considerations should not come as surprise when the number of requests is as large as that reported by Google, reaching 1.265.825 since May 2014, meaning around 35.000 per month, and above 1.200 per day.[15] With these volumes, the RTBF has a taxing effect on search engines, which now need to employ several people specialized in taking care of this type of requests. That effect is likely to increase in the future, as more information is being put online and as the awareness over the existence and the application of the RTBF is likely to increase. Growing awareness is expected as a result of the forthcoming General Data Protection Regulation (GDPR), which enshrines the RTBF in its article 17 and provides for severe fines in case of violation or non-compliance. The GDPR also raises a fundamental question of expansion of the applicability of the RTBF to social media companies and other web hosts,[16] which could seriously hamper the viability of start-up businesses by forcing them to devote significant resources to a robust legal analysis of these claims.

B-Communication to the affected publisher

Another controversial issue addressed by the A29WP Guidelines concerns communications between the search engine and the publisher affected by the delisting. The position taken in the Guidelines is that search engine managers should not, as a general practice, inform the webmasters of the pages affected by de-listing. This position is contentious because, it sacrifices transparency to prevent original publishers from re-publishing the delisted links or the content of the affected pages[17] – a practice that risks undermining the purpose of the RTBF. It also runs against Google's established practice of notifying registered webmasters of affected websites after the delisting occurred.[18]

At a more fundamental level, the position is problematic because it highlights the one-sidedness of the obligation imposed on search engines operators, who are required to adjudicate RTBF claims on the basis of the allegations of data subjects, but not to hear the original publishers in the course of that process, or inform them after the fact. This evidently raises due process concerns, as it affects the publishers' freedom of expression without granting them the right to participate in the fact-finding. The Guidelines do concede that it may be legitimate (a far cry from being required) for search engine operators to contact original publishers prior to any decision about a de-listing request, in particularly difficult cases, when it is necessary to get a fuller understanding about the circumstances of the case. However, limiting these communications to cases that appear "difficult" is a dangerously elegant solution, as it neglects that it is often precisely by hearing the other side of a story, that one can cast doubts on the accuracy

13. J van Hoboken, Search Engine Freedom. On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines (Alphen aan den Rijn: Kluwer Law International, 2012), 351.
14. E Haber, 'Privatization of the judiciary', 40 Seattle U. L. Rev. 115 (2016).
15. Microsoft reports significantly lower numbers, with 18.101 received from May 2014 to December 2016, equal to 583 per month and thus merely around 18 per day. See https://www.microsoft.com/en-us/about/corporate-responsibility/crrr/
16. For an analysis of the possible scenario, see D Keller 'The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation' Available at SSRN: https://ssrn.com/abstract=2914684.
17. For example, both the BBC and the Telegraph posted a list of removed links, which in the case of the Telegraph included details about the affected stories. See N McIntosh 'List of BBC web pages which have been removed from Google's search results', BBC (25 July 2014) http://www.bbc.co.uk/blogs/internet/entries/1d765aa8-600b-4f32-b110-d02fbf7fd379 and http://www.telegraph.co.uk/technology/google/11036257/Telegraph-stories-affected-by-EU-right-to-be-forgotten.html.
18. J Ausloos and A Kuczerawy, 'From Notice-and-Takedown to Notice-and-Delist: Implementing the Google Spain Ruling' 14 (2) Colorado Technology Law Journal, 219, 240.

of the characterization of facts (for example, the role of a person as public figure in a community).

The A29WP's position is rooted on the belief that communications of delisting requests "in many cases" involve the processing of personal data, and that there is no valid legal basis for such processing. However, the latter conclusion is debatable: processing is lawful according to article 7(e) of the Data Protection Directive (DPD) (and GDPR) when "necessary for the performance of a task carried out in the public interest", which strikes as a fitting description of the kind of responsibility imposed on search engines to balance the interest of the claimant with those of the general public. To the extent hearing the other party is necessary to ensure that facts are accurately represented in RTBF claims, this ground for processing would appear to be a task carried out in the public interest, therefore justifying the communication of information.[19]

Google recently tried to defend its webmaster communication practice to the Spanish DPA, Agencia Española de Protección de Datos (AEPD), on the basis that the communication was necessary for the legitimate interests of publishers, but the AEPD dismissed the claim contending that publishers do not have a legal right to have their contents indexed and displayed, or displayed in a particular order.[20]

Pivotal in the AEPD's decision to find the practice illegal was the consideration that the communication poses a significant risk of re-publication by original publishers, leading to the weight of the fundamental right to data protection overriding any possible legitimate interest that the communication would serve. However, it has been observed that this argument by the DPA lacks evidence, while on the other hand Google showed that the practice has actually led to a strengthening of data protection by prompting the addressees of the communication to anonymize the data in the affected page. If proved empirically, Google's assertion could perhaps support a reversal of the position so far taken by DPAs, especially if the search engine in question can show that it contractually binds publishers not to republish or further process those data.[22]

At the same time, it is worth noting that this debate over communication between different data controllers processing the same personal data for which erasure has been requested will be impacted by article 17 (2) of the GDPR, according to which "where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall 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". In other words, the legitimation seems to have turned into an obligation, although mitigated by the definition of "reasonable steps", and applicable only to cases where the controller has made the personal data public- hardly an obstacle in the case of search engines.

C-Involvement of different jurisdictional interests

A third controversial issue is the tension generated by possible conflicts of interests between jurisdictions as a result of the scope of RTBF remedies. Specifically, it seems hard to reconcile the global nature of the Internet with the national basis of delisting requests, which can nonetheless affect the ability of users in other countries to access search results. As a result, the data protection interest of the originating country may clash with the interest of other counties to protect freedom of expression and information; but also more broadly, with

19. It has also been suggested that publishers may need that information for purposes of intervening in administrative or court proceedings, and therefore this could be qualified as a legitimate interest for processing. However, this ground of processing would be significantly narrower, as limited to the cases in which the controller can initiate or intervene in legal proceedings on the basis of freedom of expression. See E Bougiakiotis, 'The Enforcement of the Google Spain ruling', 24 International Journal of Law and Information Technology, 2016, 311, 338.

20. See Resolucion R/02232/2016 in proceeding Procedimiento No PS/00149/2016, available at http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2016/common/pdfs/PS-00149-2016_Resolucion-de-fecha-14-09-2016_Art-ii-culo-10-16-LOPD.pdf. For an overview of the arguments of the parties, see D Erdos, 'Communicating Responsibilities: The Spanish DPA targets Google's Notification Practices when Delisting Personal Information', Inform Blog (21 March 2017) at https://inforrm.wordpress.com/2017/03/21/communicating-responsibilities-the-spanish-dpa-targets-googles-notification-practices-when-delisting-personal-information-david-erdos/ and M Peguera, 'Derecho al olvido: ¿el buscador puede informar a la fuente de la eliminación de un enlace', Responsabilidad en Internet (4 March 2017) at https://responsabilidadinternet.wordpress.com/2017/03/04/derecho-al-olvido-el-buscador-puede-informar-a-la-fuente-de-la-eliminacion-de-un-enlace/

21. Peguera, supra n 21.

22. The contractual obligation provides a supplementary safeguard to considered in the legitimate interest analysis, despite the fact that republication by the publisher is already likely to violate data protection rules. Whether republication may be justified on freedom of expression grounds will depend on the reconciliation between data protection and freedom of expression that is made by the relevant national law. See art 85 GDPR.

the way in which the right to data protection may be protected in the legal system of those countries.

On the geographical scope of RTBF obligations, the A29WP Guidelines indicated that delisting should be made on all relevant domains, including ".com". This clashed with the stance previously taken by Google, to limit its delisting to EU domains, which in turn aligned with the suggestions made by Google's Advisory Council on the Right to Be Forgotten.[23] Once again, Google did not have to wait long (until June 2015) to receive push-back in litigation, most notably in a proceeding before CNIL and currently pending on appeal before the Counseil d'Etat[24]. On that occasion, CNIL took the view that global delisting is the only way to guarantee that "effective and complete protection" of the data subjects explicitly sought by the CJEU.

From an international law perspective, CNIL justified the extraterritorial effects by reference to connecting factors, such as the geographical origin of the search engine user, the language used for the search and in displaying the results, and the classification of results in the list. Perhaps in recognition of the validity of the jurisdictional link, Google committed in a letter sent to A29WP during the course of the proceedings before CNIL to expand its delisting to .com domains whenever the search is conducted by a user that has been identified (through IP address) as coming from the country in which the request was made. CNIL acknowledged the improvement, but deemed it insufficient to bring Google in compliance by reasoning that IP-based solutions can be easily circumvented, and concluded that in any case "the protection of a fundamental right cannot vary depending on its beneficiary."[25]

From a coherence standpoint, the two different set of arguments made by CNIL are striking: on the one hand, the procedural justification for exertion of jurisdiction is the doctrine of effects, which constitutes an exception to the basic territoriality principle in international law.[26] Due to its exceptional nature, the effects doctrine should not be overstretched, for example extending jurisdiction in situations where the potential harm to the data subject is minimal.[27] Yet this is precisely what CNIL seems to be doing, in taking an absolutist position on the matter: according to CNIL, global delisting should apply even in cases where there is no targeting or purpose availment of the territory in question and the link with data subject is tenuous, for example simply that someone may conduct searches on the data subject from that country.

The undesirable consequences from overuse of the effects doctrine are limited by the doctrine of comity, according to which "one nation may recognize the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens, or of other persons who are under the protection of its laws."[28] However, there is no room for comity considerations in a system that predetermines the consequences to the establishment of a violation at the remedial stage: if delisting must be on a global basis, then it is not conceivable for the enforcing authority to even consider weighing the interests of other countries. A slightly more nuanced position on extraterritoriality was recently taken by the Swedish DPA, who ruled on the geographical application of delisting in deciding a series of complaints on RTBF issues[29] . Unlike CNIL, the Swedish authority does not postulate the necessity of a global remedy to ensure the fundamental right to data protection. Rather, it recognizes that the scope may vary depending on the circumstances of the case, specifically on whether there is a "specific connection to Sweden and the data subject", for example "if the information on the webpage which is linked to is written in Swedish,

23. Report of the Advisory Council on the Right to be Forgotten. Available at http://docs.dpaq.de/8527-report_of_the_advisory_committee_to_google_on_the_right_to_be_forgotten.pdf.
24. Délibération de la formation restreinte n° 2016-054 du 10 mars 2016 prononçant une sanction pécuniaire à l'encontre de la société Google Inc. Available at https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000032291946&fastReqId=273825503&fastPos=1.
25. See in this respect also the declarations made by the head of the DPA MS Isabelle Falque Pierrotin, supra n 4
26. D Svantesson, "A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft", 109 American Journal of International Law Unbound 67 (2015). See also N Zingales, Extraterritorial reach of the Marco Civil. A guide to interpretation of article 11's key criteria, <http://www.medialaws.eu/extraterritorial-reach-of-the-marco-civil-a-guide-to-interpretation-of-article-11s-key-criteria/> accessed 8 May 2017.
27. One should not confuse this statement concerning the practice of international law with the positive law of the EU, according to which "not necessary in order to find such a right that the inclusion of the information in question in the list of results causes prejudice to the data suwbject" (See *Google Spain*, para 96). Despite the incontrovertible nature of that rule, the A29WP itself recognized that evidence of such prejudice would be a strong factor in favour of de-listing. See A29WPGuidelines, p. 18.
28. *Hilton v. Guyot,* 159 U.S. 113, 163-64 (1895)). As defined in the introduction of the same paragraph, "'Comity» in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other". Id., 163.

addressed to a Swedish audience, contains information about a person that is in Sweden or if the information has been published on the Swedish domain .se".

This decision moves the debate a step forward, evoking flexibility in the application of the remedy[30], but still fails to fully account for the weighing exercise that comity principles would require. For example, what sort of remedy should the DPA impose when publication of information involving personal data of a Swedish citizen is required by law, as it was the for the auction notice in *Google Spain*? Arguably, the remedy should be designed to permit the application of that national law, as it appears required under article 85 GDPR, which attributes to Member States the task to "[…] reconcile the right to the protection of personal data…with the right to freedom of expression and information". This question is likely to become even more controversial if the prevailing interpretation of art. 17 GDPR becomes that RTBF claims can be submitted to data controllers other than search engines.

II-BETWEEN THE SCYLLA AND CHARYBDIS OF PUBLIC AND PRIVATE

The challenges highlighted so far implicate that operationalizing the right to be forgotten requires a careful design. The need to balance conflicting fundamental values, the sheer number of requests that were already filed and can be expected in the future, and the number of jurisdictions potentially affected all implicate that neither a private company nor a public agency or court can be expected to perform the job in a way that would satisfy various stakeholders and lead to socially acceptable results.

As noted above, the current EU solution whereby a private entity, notably a search engine, is asked to decide whether conditions for delisting are fulfilled while simultaneously considering the right to freedom of expression grants this entity broad discretionary powers. Both the conditions for delisting as well as the exceptions are framed in abstract terms, calling for a great degree of evaluative judgment in each instance of application. There can be real differences of view as to whether particular information is 'inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed' or to use the GDPR language 'no longer necessary in relation to the purposes for which they were collected'.[31] Even more so, there can be differences of views as to whether retaining a link is 'necessary for exercising the right of freedom of expression and information' not to mention evaluating whether the right to be forgotten is 'fair[ly] balance[ed]' against the public's right to the information. Neither the Court nor the A29WP nor the GDPR have offered much guidance on how to strike that balance.

From this perspective, a regime delegating decision-making process for delisting to search engines is problematic. Search engines cannot be just trusted to be objective in deciding whether to remove a link, because they necessarily have commercial interests tipping the scales towards delisting. At first sight, one could expect that competitive pressure should compel search engines to balance the right to be forgotten with the right to information well. After all, if they reject delisting requests too easily they may face criticism for providing insufficient privacy and data protection, as well as administrative penalties for any ascertained RTBF violations. On the other hand, however, search engines also have incentives not to delist links too lightly, because that would decrease the quality of its search results.In reality, competitive pressure cannot be expected to direct search engines towards balanced results. It is true that relevance of search results is an important quality dimension on which search engines compete.[33] However, since it is difficult to measure the quality of search results, consumers are hardly able to identify quality differences, and competitors have troubles signaling them in the market process. For this reason, it has been argued under current conditions of competition, the largest search engine has the ability and incentive to degrade the quality of its search results to the detriment of consumers . This is because network effects actually increase the dominant engine's profits when it degrades search quality by providing more 'sponsored' results at the expense of organic results. Competitive pressure in this market is limited, considering the importance of scale in this market to create a "virtuous circle" leading to continuous better results and more users.

29. Decision Tillsyn enligt personuppgiftslagen (1998:204)- Google Inc. och Google Sweden AB. Available at http://www.datainspektionen.se/press/nyheter/the-right-to-be-forgotten-may-apply-all-over-the-world/
30. In line with this approach (and proposing a more contextual balancing of interests), see B van Alsenoy and M Koekkoek, 'The Extra-Territorial Reach of the EU's 'Right to Be Forgotten'' International Data Privacy Law (2015) 5 (2) 105.
31. Article 17(1)(a) GDPR.
32. Article 17(3)(a) GDPR.
33. See European Commission Case No. COMP/M. 5727-Microsoft/Yahoo! (Feb. 18, 2010) (C 1077), para. 100.

IMPLEMENTING THE RIGHT TO BE FORGOTTEN: TOWARDS A CO-REGULATORY SOLUTION?

Similar problems can be expected with regard to the choice concerning removal of links. Like any private undertaking, a search engine is driven by its own profits rather than public policy considerations. Accordingly, we can expect that it will prefer to err on the side of caution, and delist links even when a request is not justified. Or we can expect it to accept more readily delisting requests concerning its competitors' websites (for example, a service that is equivalent to 'Google News'). Under the current system, it will be extremely hard to detect this type of overreach, and nobody would have recourse against an overzealous RTBF delisting. By contrast, the GDPR requires that those who request delisting have full knowledge whether their request has been accommodated, and provides them in case of dissatisfaction with the possibility to start a legal proceeding against the data controller.

In light of all the rehearsed arguments against delegating the implementation of delisting to private entities, one might conclude that this power should rest with a public body. However, a public body would also face significant limitations in effective administration of the right to be forgotten. As mentioned, Google alone has reported 1.265.825 requests since May 2014, meaning around 35.000 per month, and above 1.200 per day. While this has been a significant burden on Google, it would have even more paralyzing effect on a public agency disposing of a smaller budget, fewer staff and lesser expertise in processing large volumes of data in an efficient manner. We could expect a serious backlog in processing delisting requests, which would undermine the effectiveness of protection. Moreover, given the current institutional set up relating to the protection of privacy and data protection, attributing this competence in the first instance to the public sector would require the involvement of 28 DPAs with potentially significant duplicative costs (namely, in conducting the same type of analysis and dealing with similar requests), and most importantly, diverting their resources away from other important areas of enforcement of data protection law.

Since neither private nor fully public architectures appear adequate to deal with RTBF adjudication, the ideal solution is a hybrid. To that end, we propose a co-regulatory solution where search engines would serve as 'front handlers' of delisting request, while a specialized public agency would be entrusted with task of reviewing their decisions, and empowered where necessary to initiate actions for reinstatement on public interest grounds.

III. THE NEED FOR AN AGENCY FOR FREEDOM OF EXPRESSION AND INFORMATION

Scholars and policy makers have extensively discussed and developed the principles of good governance that a public-private regulatory regime needs to meet to be considered legitimate in a policy based on the rule of law and to be effective in meeting its goals. While we draw from this literature, we consider that our primary resource should be the Principles of Better Self- and Co-regulation developed and committed to by the European Commission, and the right to good administration enshrined in Article 41 of the EU Charter of Fundamental Rights. In this short paper, we simply highlight the most relevant principles and how they inform the solution we propose.

A. Principles of better self- and co-regulation

1) Participation

Participants in a self- or co-regulatory mechanism should represent as many stakeholders as possible. The requirement of broad participation aims to ensure that all relevant interests are properly represented and thus taken into account and given adequate weight in a decision-making process. This procedural safeguard is linked to a substantive concern, namely, ensuring that the affected are fairly or appropriately treated in the decision made. At the same time, procedural regard should prevent excessive influence of overrepresented interests and resulting bias in their favour.

To achieve broader and effective participation, the general public could be given proper representation in delisting decisions through the establishment of a dedicated public agency: an agency for the right to information and freedom of expression. The agency, established in each EU member state, would review delisting decisions taken by a search engine and evaluate whether they may infringe the public right to information, being empowered to verify the accuracy of the information by establishing contact with the original publishers. If the agency concludes that the public

34. M Stucke and A Ezrachi, 'When Competition Fails to Optimize Quality: A Look at Search Engines' 18 Yale Journal of Law & Technology 70 (2016)
35. N Zingales, 'Product Market Definition in Online Search and Advertising' (2013) 9 (1) Competition Law Review 29
36. See supra note 13.
37. Richard B Stewart, 'Remedying Disregard in Global Regulatory Governance: Accountability, Participation, and Responsiveness' (2014) 108 (2) American Journal of International Law 211, 224.

right to information is violated to an extent justifying legal intervention, it shall inform the claimant and the respective DPA. It shall be then up to the claimant and the DPA to decide if they agree with the agency's point of view. If they do, the agency shall request the search engine to adopt the necessary measures. However, if either the DPA or the claimant disagrees with the agency the latter would then be entitled to initiate legal proceedings in national courts to protect the public interest of the right to information and freedom of expression. The court would finally decide whether a link should be re-listed, or whether the scope of delisting should be modified.

2) Openness and transparency

Transparency means public access to decision-making process. It can involve access to actual proceedings and to the relevant documentation. Transparency is crucial for understanding the reasons behind a decision taken and facilitates controlling its correctness. Thus, transparency is crucial for accountability. In our case, transparency is crucial for public control of whether delisting decisions fairly balance the right to data protection with the right to information. It needs to be ensured at both public and private stages of decision-making. Transparency can help ensuring that both search engines and agencies adhere to their obligations.

Transparency involves a number of different mechanisms, such as the holding of meetings in public, the provision of information and the right of access to documents. As regards proper operationalization of the right to be forgotten, transparency could involve the following elements:

- Statistics about delisting requests and their treatment by search engines, agencies, and DPAs respectively;
- Statistics about the rationales for either delisting or refusing to delist;
- Categories of requests and sources , including a division by time elapsed since publication.
- A disclosure of the existence of any type of algorithm involved in filtering out delisting requests, and a general explanation of its functioning.
- Annual reports by the agencies explaining the rationale for their actions, including failure to act. In particular, the (anonymized) reports published by the agency should overtime provide guidance as to the type of requests that would justify delisting and those that would not.

3) Clear objectives

The objectives of the regulatory scheme should be set out clearly and unambiguously. In our case, the competences of the agency and the conditions under which it would be required to intervene should be specified with a certain level of precision to limit its discretion and enable accountability. If these competences are too vague, control can become elusive and both the right to data protection as well as the right to information can be undermined. Importantly, the mandate of the agency should include considering the right to freedom of expression and information in third countries that might be affected by delisting. This would enable the agency to give representation to the interests of those countries, and feed as much as possible comity principles into RTBF adjudication.

4) Financing

As the new agency would be a public body serving the public interest, it could be financed from public funds. Search engines and DPAs would however remain responsible for the processing costs on their side, namely the additional costs incurred due to litigation with the agency. While this arrangement implies at least in theory that one agency is funded to "cannibalize" the work of the other agency, the degree to which this occurs will largely depend on the legislation passed in Member States to give content to the general exception of article 86 GDPR.

B) Right to good administration

Potential intervention by the agency represents an additional level of scrutiny of delisting requests and as such it would affect the exercise of the individuals' RTBF. Given the volumes of delisting requests, some preliminary screening mechanism appears necessary to limit the number of requests reviewed by the agency, and thus improve its ability to handle reviewed cases in a timely manner and with due care.

38. See along these lines the letter signed by 80 academics requesting to Google more granular information. Ellen Goodman, 'Open Letter to Google From 80 Internet Scholars: Release RTBF Compliance Data', Medium (14 May 2015) at https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd.

IMPLEMENTING THE RIGHT TO BE FORGOTTEN: TOWARDS A CO-REGULATORY SOLUTION?

Filtering should ensure that only two types of cases are reviewed by the agency: (1) those were the right to information clearly prevails; (2) 'difficult cases', that is, requests involving a real conflict between two justified interests are reviewed by the agency. Cases where it is relatively 'clear' that the right to data protection should prevail or when the right to information is weak should be filtered out. Selection could be facilitated by:

(a) Standardized delisting request forms, including a breakdown of the type of interest invoked (as is currently the case for Microsoft Bing, but at a more granular level). Standardization actually provides an additional benefit of a "one stop shop" for claimants, which could simultaneously submit that form to any controller subject to RTBF obligations .\

(b) An obligation on search engines to classify requests into different categories (along the lines of transparency reports), and to "flag" for review cases which appear complex, or where delisting would constitute a substantial interference with freedom of expression.

(c) An obligation for search engines to establish communication with the original publisher, under confidentiality agreement, in order to verify the accuracy of the facts alleged.

(d) The possiblity for publishers and members of the general public to lodge complaints with the agency.

(e) A penalty for frivolous or meritless RTBF claims.

The ability to initiate joint actions is another way to economize on administrative resources. The agency should therefore have the power to consolidate requests of the same type.

The requirement of giving reasons for the decisions made – another element of the right to good administration – is closely related to transparency. That is, it makes the decision-making process more transparent to the affected parties, so that they can know why a particular decision has been adopted. At the same time, the obligation to give reasons disciplines the exercise of discretion, helps ensuring that various interests at stake are duly considered and nudges the decision-maker to carry out a more careful analysis. Most importantly, the obligation to give reasons would enable claimants to appreciate the weight attributed to freedom of expression and information in a particular case.

39. See also E Haber, supra n 16, 161. E Lee 'Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten' 49 UC Davis Law Review 1017, 1086

WHAT SHOULD BE FORGOTTEN? TIME TO MAKE SENSE OF ARTICLE 17 GDPR FROM THE POINT OF VIEW OF DATA CONTROLLERS

By Pieter Van Cleynenbreugel
Professor of European Union law at the Faculté de Droit, de Science Politique et de Criminologie of the University of Liège

This contribution analyses the scope of the right to be forgotten as envisaged by the GDPR from the point of view of data controllers. It argues that the scope of this right is far from clear and that different interpretations can be given to it. It therefore calls upon the responsible institutions and authorities to take a more focused position in this respect.

The Court of Justice of the European Union's recognition of a right to obtain the removal of one's personal data displayed in search engine results (Case C-131/12, *Google Spain,* EU:C:2014:317) has opened policy discussions on the conditions under which individuals' data are to be deleted by data controllers.[1] Those discussions culminated in Article 17 of the new General Data Protection Regulation 2016/679 (GDPR),[2] explicitly stating that every data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay. That right is not unconditional, as only data no longer necessary, or unlawfully collected, can be subject to such a request. In addition, to the extent that processing is necessary in the public interest, the right cannot be invoked (on the limited nature of the right, see the contribution of O. Tambou).[3]

Despite its explicit recognition, the exact scope of the right to be forgotten cannot be derived clearly from the wording of Article 17 GDPR. Indeed, even a superficial reading of that provision immediately allows two different interpretations of this right to be distinguished. On the one hand, a right to be forgotten could be read only to incorporate an entitlement to a simple erasure, i.e. the mere technical delisting of data from being displayed in search results or databases. On the other hand, a more fundamental obligation to ensure the permanent removal of one's data, a so-called "oblivion" approach could equally be envisaged in this context. Throughout the GDPR, references to both approaches can be detected simultaneously.

I-THE ERASURE APPROACH

Arguing in favour of the mere erasure approach, one could argue that the provision only speaks about the erasure of data. As such, it does not seem to impose the permanent removal of those data from the controller's processing systems. At the same time, however, Recital 65 GDPR would seem to imply that further retention of the data should be made impossible when a successful request for erasure is made.[4] In the same way, the GDPR demands that "a controller who has made the personal data public should be obliged to inform the controllers, which are processing such personal data, to erase any links to, or copies or replications of those personal data" (Recital 66). As such, the Regulation could equally be read as calling for a more extensive oblivion approach.

1 Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014]
2 Regulation 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) OJ L 119/1
3 O Tambou, 'L'Impact du RGPD sur la Mise en Oeuvre Future du Droit à L'Oubli Numérique' in Olivia Tambou, Sam Bourton (Eds.), *The Right to be Forgotten in Europe and Beyond/ Le droit à l'oubli en Europe et au-delà* (Series Open Access Book, Blogdroiteuropéen 2018) pp.95-97
4 Regulation 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) OJ L 119/1

The lack of clarity regarding the scope of Article 17 is likely to raise practical problems from the point of view of data controllers called upon to implement it in their day-to-day business practices. When called upon to apply Article 17, erasure and oblivion approaches would entail different compliance obligations for those businesses.

On the one hand, an erasure approach would merely require data controllers to have at their disposal tools ensuring that, upon request of an individual, the latter's personal data are no longer displayed. Those data could still be stored and remain on the servers of the data controller in principle for any potential future – and permitted – use or, may even have to be retained for law enforcement purposes in the context of applicable and valid data retention regulation.

II-THE OBLIVION APPROACH

On the other hand, an oblivion approach would seem to oblige data controllers to remove personal data from their servers permanently, rather than making them inaccessible. This approach presupposes that, at the request of a data subject, all relevant data are permanently removed and that technological tools have to be in place to make this happen. In that case, EU law would require an individual's commercial transaction history to be deleted entirely and permanently from an online selling platform or any other data controller. In the same way, robots or robotic devises in personal homes, which register data, could be requested to have a feature to delete all private or personal data registered as side effects of their day-to-day activities. To the extent that oblivion would be the preferred approach, businesses would or could have to put in place means to remove irrelevant personal data from their data storage automatically and ex ante, in order to comply with Article 17 GDPR. At present, it is unclear, however, to what extent such a pro-active data removal strategy is even compatible with EU and Member States' data protection and retention regulation frameworks.

One could even speculate, in this respect, that the nature of the data controller may justify the imposition of different right to be forgotten obligations on different controllers. As such, an erasure approach is considered more feasible in certain sectors such as search engines, whereas an oblivion approach is preferable in others, such as in the context of robots interacting with humans. The GDPR refrains from even hinting at the pertinence of such a distinction.

III-THE NEED FOR CLARIFICATION

In light of the foregoing uncertainty about the exact scope of Article 17 GDPR and the differing compliance consequences different interpretations of that provision entail, an interpretative communication bringing clarity regarding the scope of that provision and concrete steps to be taken for its implementation would be more than welcome. Preferably authored by the European Commission or the Working Party of Member States' data protection authorities, the communication would have to offer concrete guidance to data controllers confronted with right to be forgotten claims (for a more developed solution, see the contribution of N. Zingales and A. Janczuck.[5] If chosen as a policy option, I would even recommend the communication to make a distinction between different types of data controllers and reflect on specifically tailored "erasure" or "oblivion" steps to be taken by them, depending on their particular activities. In doing so, more specific "right to be forgotten" compliance steps could be crafted in relation to specific data protection activities engaged in by different controllers, which could help better to understand and apply the right to be forgotten as envisaged by Article 17 GDPR (see on the opportunities presented by the right, the contribution of P. Bernal).[6] In order to avoid the right to be forgotten becoming a toothless monster when the GDPR will come to apply in May 2018, now would be a good time to take such action.

5 N Zingales, A Janczuck, 'Implementing the Right To Be Forgotten: Towards A Co-Regulatory Solution?' in Olivia Tambou, Sam Bourton (Eds.), *The Right to be Forgotten in Europe and Beyond/ Le droit à l'oubli en Europe et au-delà* (Series Open Access Book, Blogdroiteuropéen 2018) pp.84-92

6 P Bernal, 'The Right To Be Forgotten as a Positive Force for Freedom of Expression' in Olivia Tambou, Sam Bourton (Eds.), *The Right to be Forgotten in Europe and Beyond/ Le droit à l'oubli en Europe et au-delà* (Series Open Access Book, Blogdroiteuropéen 2018) pp.78-83

L'IMPACT DU RGPD SUR LA MISE EN OEUVRE DU DROIT À L'OUBLI NUMÉRIQUE

par Olivia Tambou
Maître de Conférences HDR spécialisée en droit de l'Union européenne à l'Université Paris-Dauphine, PSL Research University, Cr2D

Cet article considère que l'introduction explicite du droit à l'oubli à l'article 17 Réglement Général de Protection des Données (RGPD) a une valeur ajoutée limitée en raison des compromis qui ont été nécessaires pour permettre son adoption. Cela dit, d'autres éléments introduits dans le RGPD sont susceptibles d'avoir un impact positif sur sa mise en oeuvre, comme le principe de la responsabilisation des acteurs sous le contrôle des autorités de protection dont les compétences et pouvoirs sont harmonisés. Une seule inconnue demeure, l'usage par les Etats membres de leur marge de manoeuvre pour restreindre ce droit à l'oubli numérique dans leurs lois nationales encore en cours d'adoption.

L'article 17 du RGPD consacre explicitement pour la première fois le droit à l'oubli numérique à l'échelle de l'Union européenne. L'analyse de la génèse de cet article permet de mieux saisir pourquoi il n'a en réalité qu'une valeur ajoutée limitée (I). Cette première constatation doit néanmoins être replacée dans le contexte général des apports de la réforme envisagée. D'autres dispositions du RGPD permettent d'augurer d'un renforcement attendu de la régulation du droit à l'oubli numérique tant par les responsables de traitement que par les autorités de protection des données (II). En outre plusieurs éléments permettent de présager d'un renforcement attendu du controle juridictionnel du droit à l'oubli numérique (III). Une seule inconnue demeure. L'usage par les Etats membres des marges de manoeuvres laissées par le RGPD viendra t-il limiter la mise en oeuvre de ce droit l'oubli numérique? (IV).

I-LA VALEUR AJOUTÉE LIMITÉE DU COMPROMIS DE L'ARTICLE 17 RGPD

Le terme de « droit à l'oubli » est cité explicitement trois fois dans le RGPD[1]. Plusieurs contributions antérieures ont rappelé que la reconnaissance du droit à l'oubli à l'article 17 RGPD ne permettait pas de clarifier pleinement sa nature[2] et l'étendue des obligations qu'il comporte pour les responsables de traitement. S'agit-il d'une composante spécifique du droit d'effacement ou ce droit est-il d'une nature différente allant au-delà de l'effacement?[3] Les ambiguïtés de la formulation définitive retenue témoignent des lignes de tensions entre les co-législateurs[4]. Le Parlement européen (PE) s'est opposé au maintien de cette référence au droit à l'oubli considérant qu'il s'agissait d'une forme de droit d'effacement et que l'oubli numérique était un concept ni réaliste, ni souhaitable. Le Conseil a été favorable au maintien de cette référence à l'oubli au moins dans le titre de l'article 17. Selon lui, l' obligation pour le responsable ayant rendu publiques les données personnelles d'informer les autres responsables de traitement des demandes d'effacement justifiait en soi l'existence d'un réel droit à l'oubli. Cette seconde obligation serait l'élément clé permettant de distinguer le droit à l'effacement du droit à l'oubli et du droit d'opposition[5]. Cette utile précision permet certes, de répondre aux interrogations actuelles rencontrées dans la mise en œuvre du droit au déréférencement suite à l'arrêt *Google Spain*, sur l'existence d'une telle obligation d'information pour les moteurs de recherche[6].

Néanmoins, son acceptation a été entourée de telles précautions que sa valeur ajoutée peut apparaître limitée. D'une part, elle n'a de sens qu'à la condition de considérer qu'un moteur de recherche peut être un responsable de traitement « ayant rendu publiques » les

1. cf. Considérant 65, 66 et le titre de l'article 17.
2. Voir en particulier les propos introductifs d'Olivia Tambou p.22, et les contributions d'Enrico Peuker p.37

3 cf. contribution de Pieter Van Cleynenbreugel p.93
4 cf. notre tableau comparatif des différentes versions de l'article 17 RGPD mis en Annexe 2.
5 cf. Réunion du 24 Avril 2015 p. 3 accessible à http://data.consilium.europa.eu/doc/document/ST-7978-2015-INIT/en/pdf
6 voir contribution de Miquel Peguera, The application of the Right to be Forgotten in Spain, p.33

données personnelles. Ce point est discutable. Un moteur de recherche facilite l'accès à des données personnelles rendues publiques par l'éditeur à l'origine de leur mise en ligne. D'autre part, cette obligation n'est pas absolue. Le responsable de traitement est simplement tenu de montrer qu'il a pris des mesures raisonnables, tant du point de vue technique, que financier pour informer les autres responsables de traitement. C'est sans doute une bonne chose, car les autres responsables du traitement ne sont pas toujours identifiables. En outre, il n'est pas clairement dit que cela implique, une obligation spontanée d'effacement pour les autres responsables de traitement informés, sans requête en ce sens de la part de la personne concernée. Enfin et surtout, cette obligation d'effacement ne s'applique pas dans différentes hypothèses décrites à l'article 17§3 qui rendent le traitement de ces données nécessaires. L'obligation d'effacement sera donc variable en fonction du statut du responsable de traitement. Ainsi, comme actuellement, elle pourra jouer pour un moteur de recherche, mais être exclue pour l'éditeur originel, soit en raison d'une obligation légale, ou de l'exercice de son droit à la liberté d'expression et d'information[7] ou de la finalité du traitement (motifs d'intérêts publics variés tels que la santé, la recherche scientifique etc.). L'extension de ce droit à l'oubli aux réseaux sociaux est aussi une question qui n'est pas directement tranchée par l'article 17.

La complexité, les ambiguïtés de la formulation retenue à l'article 17 RGPD invitent donc à prendre en compte d'autres innovations pour mesurer la valeur ajoutée du RGPD pour la mise en œuvre du droit à l'oubli.

II- LE RENFORCEMENT ATTENDU DE LA RÉGULATION DU DROIT À L'OUBLI

L'un des apports du RGPD est de renforcer toutes formes de régulation. Premièrement, le RGPD introduit le principe de la responsabilité (*accountability*)[8], des responsables de traitement et de leurs sous-traitants. Cela signifie qu'ils doivent prendre des mesures pour documenter leur mise en conformité aux obligations qui leur incombent en vertu du RGPD. Cela inclut la manière dont ils entendent mettre en œuvre le droit à l'oubli, tel qu'introduit à l'article 17 RGPD. L'activité des futurs délégués à la protection des données personnelles, l'analyse d'impact relative à la protection des données comporteront nécessairement des éléments sur le traitement du droit à l'oubli. D'autres nouveautés sont étroitement liées à la volonté de répondre en amont au besoin social inhérent au droit à oubli numérique. Tel est le cas des principes de la protection des données dès la conception et de la protection des données par défaut[9]. Les outils rénovés, tels que les codes de conduites[10] pourraient aussi être adoptés pour répondre à certaines difficultés sectorielles du droit à l'oubli. Une telle éventualité pourrait être la bienvenue dans le secteur des éditeurs de presse notamment en raison des nombreux cas liés aux services d'archivage en ligne des organes de presse.

La mise en œuvre du droit à l'oubli est aussi au cœur d'une régulation institutionnelle, celle menée par les autorités de protection des données . L'harmonisation de leurs compétences, missions et pouvoirs aura un impact certain sur la future mise en œuvre du droit à l'oubli. Le RGPD confère à chacune des autorités de protection des 28 États membres :

- le pouvoir d'ordonner l'effacement des données au sens de l'article 17 du RGPD[11],
- des pouvoirs d'enquête, voire d'audit conjoint, qui pourraient être utilisés afin de coordonner des mesures de contrôle de la mise en oeuvre du droit à l'oubli par un responsable de traitement entre les autorités de plusieurs États membres[12] et de renforcer les actuelles possibilités d'inspections nationales[13].
- la possibilité d'imposer aux responsables de traitement des amendes administratives pouvant atteindre le montant le plus élevé, en cas de violation de ce droit à l'oubli (20 millions d'€ ou 4% du chiffre annuel mondial)[14].

Quant au Comité Européen de la Protection des Données (CEPD), il lui est demandé explicitement de publier des lignes directrices sur « les procédures des suppressions de liens vers des données à caractère personnel, des copies, ou des reproductions de celles-ci existant dans les services de communication accessible au public»[15]. Le droit à l'oubli devrait devenir un sujet régulier de l'interrégulation disciplinaire, c'est-à-dire entre autorités de protection des données des États membres.[16]

7 . cf. nos propos sur l'arrêt de la Cour de Cassation française du 12 mai 2016 dans notre contribution sur trois enseignements de la mise en oeuvre juridictionnelle française de l'arrêt *Google Spain.*
8 article 24 RGPD
9 article 25 RGPD
10 article 40 RGPD
11 article 58.1g) RGPD
12 article 62
13 cf. une illustration récente en Suède évoquée dans la contribution de Patricia Jonason, p.63
14 cf. article 83§5,b)
15 cf. arrticle 70 §1 g) RGPD
16 Sur ce concept d'interrégulation voir notre article dans les

L'IMPACT DU RGPD SUR LA MISE EN OEUVRE DU DROIT À L'OUBLI NUMÉRIQUE

Le renforcement du rôle et des pouvoirs des autorités de protection des données personnelles s'est accompagné d'un affermissement de leur responsabilité dans le traitement des demandes des personnes concernées. Ainsi, les autorités qui ne seraient pas diligentes pour répondre aux demandes de droit à l'oubli non exaucées par un responsable de traitement pourraient faire l'objet d'un recours juridictionnel[17]. En effet, l'article 77 leur fait obligation de tenir informé tout requérant de l'état d'avancement de sa demande.

III. LE RENFORCEMENT ATTENDU DU CONTRÔLE JURIDICTIONNEL DU DROIT À L'OUBLI

Plusieurs éléments augurent d'une augmentation possible des contentieux juridictionnels autour du droit à l'oubli. Il est possible d'en dresser une liste non exhaustive :

• L'harmonisation des possibilités de recours prévue au chapitre VIII du RGPD,

• l'augmentation du montant des sanctions,

• la visibilité croissante du droit européen de la protection des données,

• les difficultés de mise en œuvre évoquées notamment dans les rapports nationaux du droit au déréférencent présentés dans la première partie de cet ouvrage,

• Le maintien d'une marge de manœuvre importante des États membres en raison du caractère de règlement incomplet du RGPD. Il existe une cinquantaine de clauses dites ouvertes permettant aux États membres de maintenir, d'introduire des dispositions plus spécifiques, des dérogations à des droits. L'usage de ces clauses ouvertes augure des besoins d'interprétations qui sont susceptibles de porter sur la mise en oeuvre du droit à l'oubli et qui relèveront de la compétence des juges. Cela ressort explicitement de l'articulation entre l'article 17 §3 qui permet aux États membres d'introduire des obligations légales du maintien de certains traitements ne pouvant faire l'objet d'un droit d'effacement et d'oubli et de l'article 85 RGPD, qui leur donne une compétence pour légiférer sur l'articulation du droit à l'oubli avec la nécessité de maintenir les traitements concernés en raison de leur finalité.

IV. LE MAINTIEN NÉCESSAIRE DE LA MARGE DE MANŒUVRE DES ETATS MEMBRES

Lors des discussions au Conseil, l'Allemagne[18] avait proposé la possibilité de mettre en place un mécanisme de règlement des différends spécifique pour les moteurs de recherche. Cette éventualité a été rejetée. Le fait qu'un tel mécanisme aurait eu pour principal objet d'établir la balance des intérêts entre droit à l'oubli et liberté d'expression et d'information en est la cause[19]. Cela atteste de la volonté des Etats membres de rester maîtres de cette articulation, comme l'illustre clairement l'article 85 du RGPD. L'article 9 de la directive 95/46 autorisait déjà les États membres à prévoir des dérogations pour le traitement des données personnelles aux seules fins de journalisme ou d'expression artistique et littéraire[20].

La formulation de l'article 85 RGPD est plus ouverte. Il s'agit de permettre aux États membres de concilier le droit à la protection des données personnelles et le droit à la liberté d'expression et d'information y compris le traitement à des fins journalistiques et non plus seulement des traitements à finalité exclusivement journalistique. En outre, un élément nouveau « les finalités d'expression universitaire » peut être pris en compte par les Etats. Les débats que suscite le récent projet de loi allemand[21] visant à demander l'effacement des propos haineux et délictueux prononcés sur les réseaux sociaux témoignent d'une évolution possible. La volonté d'endiguer le phénomène dit des « fakes news » renouvelle les problématiques anciennes liées au caractère très culturel de la liberté d'expression. La prise de conscience des dangers de la diffusion massive de contenus sur internet *via* les plateformes pourrait amener les législateurs nationaux à opérer une conciliation entre droit à l'oubli et liberté d'expression moins généreuse pour la liberté d'expression sur ces canaux.

Mélanges Joël Monéger sur L'émergence d'un modèle européen d'interrégulation en matière des données personnelles, Mai 2017
17 cf. article 78§2 RGPD

18 cf. doc accessible à http://www.statewatch.org/news/2015/feb/eu-council-dp-reg-right-to-be-Forgotten-dispute-settlement-6032-15.pdf
19 cf. document accessible à http://data.consilium.europa.eu/doc/document/ST-7526-2015-INIT/en/pdf p. 4
20 Pour une illustration de l'usage actuel de ces possibilités cf. Cristina Pauner Chulvi, La actividad periodística en los ordenamientos nacionales y europeo sobre protección de datos in Hacia un nuevo derecho europeo de protección de datos, editores Artemi Rallo Lombarte y Rosario García Mahamut, Tirant Lo Blanch, 2015 p. 571-619
21 Jan Mönikes #NetzDG und #DSGVO – droht der Meinungsfreiheit in Deutschland ein "perfekter Sturm"?, Telemedicus, 22 April 2017

THE ROLE OF JUDICIAL DIALOGUE BETWEEN THE CJEU AND THE ECTHR IN THE FORMULATION OF THE RIGHT OF PRIVACY

By Dr. Konstantinos Margaritis
Adjunct Lecturer, Department of Political Science, University of Crete, Attorney at Law, member of the Governing Board, Hellenic Association of Public Law

Google Spain **is a landmark decision for a variety of reasons. In particular, the CJEU has outlined the framework of the right to privacy, from the personal data protection perspective, in the case of conflict with the freedom of information mainly, and expression subsequently. This being the case, the Court favored the former over the latter in principle, setting at the same time the prerequisites for the rebuttal of this presumption. On the other hand, the ECtHR has dealt with matters of conflict between right to privacy and freedom of expression (including information) to the point that we can speak of a corpus of decisions setting the parameters for a balance between the two. In that regard, a case similar to** ***Google Spain*** **is pending before the ECtHR (M.L. v Germany and W.W. v Germany). In this post, the impact of judicial dialogue between the two major European Courts will be highlighted in the formulation of the right to privacy on a pan-European level.**

I-INTRODUCTORY POINTS

In the era of information technology and extensive use of the internet, the right to privacy has faced new challenges. Taking a traditional view on the matter, Warren and Brandeis had, from 1890, emphasized the necessity of privacy for every person; the right to be let alone.[1] In principle, as defined in both Article 7 and 8 (the more specific aspect of privacy) of the EU Charter and Article 8 ECHR, the right to privacy conflicts with other rights of a fundamental nature, including those of expression and access to information.

In *Google Spain*, the CJEU generally presumed the primacy of the right to privacy over the right of internet users to have access to information. That presumption, however, can be rebutted on the grounds of the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life (par. 81, 97). This will be judged on a case by case basis.

The CJEU set two main criteria under which the access to information concerning personal data may override the right to privacy: the nature of the information at stake and the role played by the data subject in public life. Applying those criteria in the examining case, the CJEU concluded that the right to privacy prevailed.

II-THE APPROACH OF THE STRASBOURG COURT

Although there is no specific provision protecting the right to personal data in the ECHR, the Strasbourg Court has repeatedly extended the scope of Article 8 ECHR to include the concept of personal data.[2] Indeed the Court has referred to personal data as of fundamental importance to the enjoyment of the right to privacy.

With reference to the conflict between the right to privacy and freedom of expression, from the perspective of information disclosure, the Court has developed longstanding principles, which it applies to the particular facts of each case.[3] In the recent case of *Axel Springer SE and RTL Television v Germany* (app. no. 51405/12), it further clarified the principles that

1 S. D. Warren, L. D. Brandeis, "The Right to Privacy", *Harvard Law Review*, Vol. IV, No. 5, 1890, available at http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm

2 *S. and Marper v the United Kingdom,* app. nos. 30562/04 and 30466/04; *Flinkkilä and Others v Finland*, app. no. 25576/04; *Saaristo and Others v Finland*, app. no. 184/06.

3 Among others, *von Hannover v Germany (no. 2),* app. nos. 40660/08 and 60641/08; *Peck v the United Kingdom,* app. no. 44647/98; *Reklos and Davourlis v Greece,* app. no. 1234/05

could lead to restriction of the right to privacy. They could be categorized as follows: those referring to the person himself (public figure, voluntary exposition), those referring to the contribution of the personal data to a debate of public interest and finally those referring to the content, form and consequence of the publication (par. 43-54).

What should be underlined at this point is the parameter of consequences of such publication and its storage, as a driving force in the reasoning of both Courts' decisions. Although not explicitly mentioned in *Google Spain*, the right to be forgotten reflects the will of the person to erase certain negative moments of his life which can still have consequences on social perceptions, leading to possible prejudice towards that person. The widespread dissemination of such information through the internet inevitably perpetuates those consequences at a social level.

In addition, cases concerning the storage of personal data on public databases have been discussed before the Strasbourg Court.[4] The result demonstrates the strong will of the Court to protect that aspect of the right to privacy, since it has pointed prerequisites under which private data can be retained. First, a mechanism that ensures non-disclosure of individual's private data must exist as well as a real possibility of deletion upon request, through a formal procedure.[5] Additionally, the Court emphasized the duration of the storage, which should be reasonable. However, the specific characteristics of the case will be considered, which may lead to extensive public interest.[6]

III-CONCLUDING REMARKS

From the aforementioned, a high level of coherence in the case law of the major European Courts can be extracted as a result. Both the CJEU and the ECtHR have explicitly identified the importance of the right to privacy, especially the new challenges that it faces in the internet era where private information spreads faster than ever and storage of private data lasts longer than ever. This identification also came through the prerequisites for lawful restriction, which must represent an important matter of public interest in line with the nature of the information provided and the role of the person affected.

The impact of such coherence is extremely significant for the formulation of the right to privacy in Europe. First of all, for the EU *stricto sensu* since both Articles 7 and 8 of the Charter refer to Article 8 ECHR in the relevant explanations and therefore those rights shall have the same meaning and scope as the corresponding provisions of the ECHR, but more substantially, in a pan-European dimension, the two legal orders comprise important elements of composite constitutionalism in Europe. Therefore, a common formulation clarifies that matter to a high extent by establishing common principles in which the member states will base protection of privacy at the internal level.

Finally, the level of coherence among the Courts will be further elucidated in the pending case of *M.L. v Germany and W.W. v Germany* before the Strasbourg Court. Relevant to the right to be forgotten, the case concerns two citizens who have served criminal penalties (released now for 10 years) and were refused the anonymity of their personal details, which appear in news websites from the time of the trials.

4 European Court of Human Rights, Research Division, *Internet Case Law and the European Court of Human Rights,* available at http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf.
5 *M.M. v the United Kingdom*, app. no. 24029/07; Brunet v France, app. no. 21010/10.
6 For example the seriousness of the crime, B.B. v France, app. no. 5335/06.

Partie 3 : Le droit à l'oubli au-delà de l'Union européenne
Part 3: The Right to Be Forgotten beyond the EU

SHEDDING LIGHT ON THE RIGHT TO BE FORGOTTEN IN RUSSIA

By Cyril Cohendy
PhD student at the Université Paris 1 Panthéon-Sorbonne on a mission to the French University College of St. Petersburg.

Russian lawmakers claimed they established the right to be forgotten according to the European practice as set up in the case *Google v. Castejo*. This statement is misleading. The law 264-FZ passed in July 2015 provides indeed the right for delisting URL links on rather broad terms but it does not seek out a fair balance with the right to access information. Therefore, the right is left to the users' own will who must prove their claim towards search engine operators. About three years have gone since the law came into force, and despite case law studies, the effects of the right to be forgotten are unquantifiable, mainly due to a lack of statistics from search engine operators.

The Federal Bill 264-FZ of the 13th of July 2015[1] introduces three amendments to the Federal Law 149-FZ on information, information technologies and data protection as well as two others to the civil procedure code. This Bill entered into force on the 1st of January 2016 and the relevant provisions for our topic were added to the Law 149-FZ in the new article 10.3, which provides conditions for delisting, and completed Article 2 as it regards search engine definition.[2][3]

In fact, these amendments established a right to delisting rather than a right to be forgotten. They are inspired by the "European practice" following the judgment of the Court of Justice of the European Union in the case *Google v. Costeja*.[4] Even, according to the law project, this Bill complies with this so-called European practice[5].

A similar design to that set by the CJEU is indeed noticeable, however great discrepancies rapidly emerge in their elaboration. The Bill allows individuals[6] to demand the *deletion* of URL links appearing on a

1 Федеральный закон N 264-ФЗ от 13 июля 2015 О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации (Federal Bill 264-FZ of the 13th of July 2015 on the modification to the Federal law relative to information, information technologies and data protection).

2 Федеральный закон от 27 июля 2006 года N 149-ФЗ Об информации, информационных технологиях и о защите информации.

3 For a full translation in English and an analysis with regard to the CJEU case *Google v. Costeja* : Nurullaev R.T. (2015) Right to Be Forgotten in the European Union and Russia: Comparison and Criticism, *Pravo Zhurnal Vysshey shkoly economiki*,_n°3, pp.181–193; Available at https://www.hse.ru/data/2015/10/11/1076267685/nurullaev.pdf, (accessed on the 18/03/2018)

4 CJEU, case C131/12 *Google Spain v. M. Costeja*, 13/05/2014, Great Chamber, ECLI:EU:C:2014:317.

5 "Представляемый законопроект согласуется с общеевропейской практикой решения аналогичных вопросов" ("The proposed law projet is pursuant to the European decision practice on analogue questions"). See: Пояснительная записка от 25 мая 2015 г. к проекту федерального закона О внесении изменений в Федеральный закон Об информации, информационных технологиях и о защите информации и отдельные законодательные акты Российской Федерации, Explanatory note on the federal law project relative to the modification of the law federal on information, information technologies and data protection, 29 may 2015, http://sozd.parlament.gov.ru/download/D7B2ACE3-50EC-4018-BEBA-B39F4D6E62B4 , p. 8 (Accessed on the 19/03/2018).

6 At the moment it is not clear whether this Bill is addressed to individuals or to Russian citizens. Overall critiques on the vocabulary, scope of the Bill and definition of the terms were raised by lawyers and academics, see for instance : Т.А. Полякова, Заключение На проект ФЗ № 804132-6 «о внесении изменений в ФЗ «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации» ; на проект № 804140 -6 «О внесении изменений в Кодекс РФ об административных правонарушениях» 2015, http://www.igpran.ru/public/publiconsite/Zaklyuchenie_IGP_RAN_Pravo_na_zabvenie.pdf (accessed on the 19th of March 2018).
Also in the following case, the plaintiff's allegations on the ground of art. 10.3 of the Law 149-FZ seems to be admissible whereas request was sent on behalf of a company, see Решение № А40-79421/17-148-446 от 3 Июля 2017 г. Арбитражный суд города Москвы (АС города Москвы) - Case A40-79421/17-148-446 of the Arbitration Court of Moscow on the 3rd of July 2017.

THE RIGHT TO BE FORGOTTEN IN RUSSIA

search engine as a result of a search based on their name. Operators are bound to comply with such requests when links give access:[7]

- To information about the applicant *distributed* in breach of the Russian legislation;
- To inaccurate information[8] and;
- To irrelevant[9] information, having lost its relevancy due to subsequent information or events.

Two exceptions follow – links cannot be delisted if they report on criminally punishable acts whose statutes of limitations have not yet come to a term, nor if they contain information on the conviction of a crime which has not entirely been served.

In comparison with the so-called European practice, at first reading, this Bill mainly fails to mention two principles raised by the CJEU. The objective underpinning this Bill was to provide a predominant and an expeditious right to privacy,[10] yet peculiarly as a result no balance has been struck either with the freedom of expression including its corollary, the public interest to information, or with the economic interest of search engine operators. Though these fundamental rights are enshrined into, for instance, the Constitution of the Russian Federation, the legislator merely ignored them when drafting the legal test that operators are charged with administering for requests. Therefore, in the spirit of the text, operators should strictly read the legislator's instructions. However, feedback and case practice show that formal criteria set in the Bill miss the legislator's presumed target. Notably, rights of third parties and the economic interest of search engine operators are necessarily taken into account during delisting proceedings and before courts by operators and judges (I).[11] Nonetheless, it is unclear how much room to manoeuver jurisdictions have in relation to taking into account the freedom of expression and the right to access information (II).

I-AN UNDEFINED LIABILITY ON THE PART OF OPERATORS TO PROCEED

At first glance, the main tasks are assigned to search engine operators. When receiving electronic, or epistolary, requests including mere personal details and URL-links, they are tasked with determining whether these breach one of the three main conditions set by the Bill within the next ten working days. This is comparable to an investigation aiming to establish the grounding of allegations from presumed facts brought by the applicant compared to the content of third parties' websites. In this task, claimants are to provide evidence of their plea and, within this period, operators may ask for further details if it considers the claim insufficiently grounded. This prolongs the proceeding for another ten-working days, during which the applicant has to reply. Eventually, the operator must justify any refusal to delist URLs.[12]

Also, it is not clear whether the law provides the operator with a mandate to delist only specified URLs by the applicant, or any other link transmitting the mentioned unlawful, inaccurate or irrelevant information. Indeed, the first point of Article 10.3 provides that the operator shall remove links of the aimed website pages allowing access to information about the applicant. On the other hand, point 5 suggests that the operator shall remove links on the information, such as indicated in the applicant's request in response to searches made on the basis of the applicant's name. Therefore, this implies that the operator would be liable for similar

7 Supra note 2, Art. 10.3 point 1, Federal law N 149-FZ.
8 Sometimes translated as "incorrect", see supra note 3.
9 Sometimes translated as "obsolete", see infra note 16 or "irrelevant" see infra note 13.
10 For instance, in the law project, proceedings were to last 3 days: see supra note 5, p. 4.
11 See Press release of the Committee on information policy on the 11/06/2015 "11 июня 2015 года состоялось заседание Комитета Государственной Думы по информационной политике, информационным технологиям и связи", http://www.komitet5.km.duma.gov.ru/Novosti-Komiteta/item/20022/ (Accessed on the 18th of March 2018). The President of the Committee remarks: "There (in the European Union) the Court of justice took the decision allowing any citizen or resident of the EU to address to search engine operators for deleting irrelevant information. It doesn't matter whether it is bad or good information, when irrelevant they are deleted. Another consideration is the possibility of a pre-trial settlement of dispute. We can compare it with the law on antipiracy where experience shows that majority of claims are resolved in court. The proposed measure will not lead to silence information about public figures. It remains to court to reach a final decision on such matters. This is not a law for Members of the Parliament, but for simple consumers. This is peculiarly true for young consumers of the Internet, for whom, unfortunately, virtual reality in some cases happens to be more important than everyday reality. The growing topic of "cyber-humiliation", even such a special term appeared, can be limited by excluding some information about events from the user's life childhood or obsolete ones. This can also serve, among other things, to prevent young people from committing suicides, which are the result of cyber-humiliation".
12 It appears from analysed case law that the provided justification for refusal binds operators during litigation.

THE RIGHT TO BE FORGOTTEN IN RUSSIA

information to that pointed out by the applicant.[13] However, for the moment, trial jurisdictions tend to rely on results of research based strictly on the name of the applicant and on links conveyed to the operator during the proceeding.[14]

Despite the criteria's broadness, according to statistics, during the first quarter of the year 2016, only 27% of 3600 requests to Yandex were successful, with Yandex being the most popular search engine in Russia.[15] I may underline that since then there are no other relevant statistics available.[16] This low percentage seems to be the result of short deadlines and of the formal terms of the law.[17] Indeed, by excluding a legal test based on public interest, the conclusion of the legal reasoning depends on evidence and fact checking of presumed inaccurate or irrelevant information as well as on a legal demonstration that such information breaches the Russian legislation.[18]

One may think that these conditions discourage some to proceed further. Before first instance courts, it appears that refusals from operators to delist aimed links are effectively based on formal grounds, such as insufficiency from applicants in providing tangible evidence.[19] Above all, these considerations may readily fall to the competence of the judge, who alone may pursue such an investigation while guaranteeing respect to the third parties' rights. As a matter of fact, when analysing the accuracy of the aimed information, Russian jurisdictions tend to require that a breach of the right to expression of third parties shall have previously been assessed by a judgement on this specific case. In addition, this would require a ruling on a presumed breach to honour, reputation and dignity, which is prescribed by other procedures within the Russian legal system.[20]

In any case, passivity or refusal from the operator allows the applicant to bring its claim before a court, which may impose a fine ranging from 100 000 roubles (1500 Euro) up to a Million roubles for repeated infringements. With regard to the frequency of requests, these amounts were deemed to be punitive by the Supreme Court of the Russian Federation.[21]

Regarding the identification of search engine operator liability for proceeding with a request, based on Article 10.3 of the Law 149-FZ, it must be firstly noted, that the material scope of the law is undefined. The legislator encompasses as search engine operator, those whose activity is to *diffuse to consumers* situated on Russian soil publications and advertising through the Internet.[22] District courts rightly raised the point that such a service does not diffuse information but retrieves it.[23] This has a direct impact on the spatial scope. For

13 Article 19, "Russia: The "Right To Be Forgotten" Bill", Free word centre, August 2015, p. 16. https://www.article19.org/data/files/medialibrary/38099/Full-Analysis---Russia---RTBF-Final-EHH.pdf (Accessed on 18/03/2018)

14Решение n°2-7072/2016 от 2 Ноября 2016 г., Московский районный суд, Чебоксары (Чувашская Республика), Case N°2-7072/2016 on the 2nd of November 2016, district tribunal in Tcheboksary.

15 Yandex do not provide up to date surveys, see : Блог Яндекса, "О применении закона «о праве на забвение»", 25 марта 2016, https://yandex.ru/blog/company/o-primenenii-zakona-o-prave-na-zabvenie (accessed on the 17/03/2018).

16 Microsoft indicates that it delisted 67% of 28 URLs requested during the first semester of 2017, See: Microsoft, Content removal request report, June 30, 2017, https://www.microsoft.com/en-us/about/corporate-responsibility/crrr (accessed on 17/03/2017) ; Google did not communicate on this matter, its report on transparency does not include Russia and it plainly does not intend to, see Theo Bertram and others, "Three years of the Right to be Forgotten", Transparency report, Google, February 26, 2018, https://drive.google.com/file/d/1H4MKNwf5MgeztG7OnJRnl3ym3gIT3HUK/view , p. 3.

17 See supra note 15.

18 See for instance: Решение N°2-2132/2017 от 23 августа 2017 г., Ленинский Районный суд, Воронежа, Воронежская область (Case N°2-2132/2017 on the 23rd of August 2017 by a district tribunal of Voronej) where the decision points out the necessity to provide certification of evidences presented by the plaintiff.

19 See Рещение N°2-3329/2016 от 5 мая 2016 г. Первомайский районный суд, Омска. (Case N°2-3329/2016, Mai 5, 2016, district tribunal of Omsk). This case is peculiarly interesting as the court recalls the right to information enshrined in the Constitution and the necessity in view of the right of third parties and the economical interest of the operator that the plaintiff shall provide irrefutable evidences, which only would allow to override such rights.

20 See for instance: Решение N°2-5158/2016 от 11 октября 2016 г., Пушкинский Районный суд, Санкт-Петербург (Case N°2-5158/2016 on the 11th of October 2016, district tribunal of Saint Petersburg) ; Решение N°2-2715/2017 от 6 апрелья 2017, Одинцовский городской суд, Московская область(Case N°2-2715/2017 on the 6th of April 2017, District tribunal, Region of Moscou).

21 Мария Макутина. "Верховный суд раскритиковал закон о «праве на забвение»", Политика, РБК, 04/08/2015, (Maria Makutina, "The Supreme court criticised the law on the right to be forgotten", politika, RBC, 04/08/2015) https://www.rbc.ru/politics/04/08/2015/55c0ba059a7947ba34f83d6c (accessed on the 17/03/2018).

22 Law 149-FZ art. 10.3, point 1 : Оператор поисковой системы, распространяющий в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации (...) : "Operator of a search engine, diffusing on the Internet advertising that is directed to the attention of consumers situated on the territory of the Russian federation, (...)".

23 Решение N°2-5158/2016 от 11 октября 2016 г., Пушкинский Районный суд, Санкт-Петербург (Case N°2-5158/2016 on the 11th of October 2016, district tribunal of Saint Petersburg); "Учитывая изложенное выше, суд пришел к выводу, что поисковый сервис ООО «Мэйл.Ру» не осуществляет распространение информации, а предоставляет пользователям услуг и поиска информации, размещенной третьими лицами в сети «Интернет», что исключает

example, the legislator did not provide indications as to whether operators are only liable for domain names "ru.", or whether legal entities are liable for proceeding requests. Peculiarly, service operators able to delist URLs are not always situated on the territory of the Russian federation and their subsidiaries cannot be held liable on this ground.[24]

Secondly, the Law 264-FZ added a definition on the meaning of search engine in Article 2 point 20 of the Law 149 FZ. This is understood as "an information system which searches for information with a certain content on the Internet network at a user's request, and provide the user with the links to website pages on the internet network allowing access to the requested date, which is stored on the Internet websites belonging to other persons, *save for* the information systems used for the performance of State and municipal functions, provision of State and municipal services and implementation of other public powers established by the Federal laws."[25]

As demonstrated by case law, only search engines provided by e.g. Google or Yandex were questioned before the court. It is still not clear what should be understood as an information system and which entities are liable, but on this ground operators were able to dismiss their obligations foreseen by Article 10.3 of the Federal law 149-FZ.[26] However, the exception concerning state performance raised by the definition of information system indicates *a contrario* that the legislator did not intend to restrain whatsoever the extent of its intervention.

II-UNFORESEEABLE EFFECTS ON THE ACCESS TO INFORMATION

Whatever it may be, the Bill on the right to be forgotten encourages individuals to send a request for the sake of her or his own will. Due to the lack of balance with the public interest to information, the three criteria – information disclosed in breach of the Russian legislation, or inaccurate or irrelevant – are tailored to the applicant's discretion.[27]

Furthermore, privacy is protected by the very fact that operators are forbidden to disclose information on requests. This means at once that they cannot divulge to third parties neither the applicant's identity, nor which URLs, giving access to their pages, were to be removed from the search engine results. Also, it is unclear to what extent and on what considerations operators can divulge statistics.[28] However, as pointed out earlier, no statistics were communicated from Yandex since the first quarter of 2016. Google merely chose not to communicate, or even to address, the issue.[29] In my view, this is most unfortunate as this is perhaps where a transparency report would be particularly useful.

Indeed, critics point out that, on the contrary, such statistics on the volume and the legal basis of requests should be disclosed so as to understand the consequences of the right to be forgotten on the freedom of expression and on the right to access information. In the same order, information of a public interest disclosed in the media may fall within the Bill's criteria, peculiarly with regard to information disclosed in breach of the Russian legislation, which has direct impacts on journalistic investigation.[30]

For instance, on the 30th of May 2016 the media RosBusinessConsulting revealed that on the request of the famous businessman Sergueï Mihaïlov, Google

возложение на ответчика ответственности за содержание информации, размещенной иными лицами": "Taking into account the above, the court concluded that the search service of «Mail. Ru» LLC does not disseminate information, but provides users with services and retrieval of information posted by third parties in the Internet, which excludes the responsibility of the defendant for the content of information, placed by other persons".

24 See the interpretation on the territoriality of the law of a district tribunal in Saint-Petersburg: Решение № 2-5503/2016 от 6 декабря 2016 г. по делу № 2-5503/2016, Пушкинский районный суд (Город Санкт Петербург) (Decision no. 2-5503/2016 of the 6 december 2016, case no. 2-5503/2016, district tribunal of Saint Petersburg) : Таким образом, суд приходит к выводу, что ответчик ООО « Гугл » не является оператором поисковой системы « Гугл », не осуществляет администрирование сервиса Google, в связи с чем не имеет доступа к сервису Google и технической возможности каким-либо образом влиять на информацию, размещенную в сети Интернет, в том числе удалять поисковую систему ссылок на веб-сайт, проиндексированный поисковым сервисом «Веб- поиск » : "Thus, the court comes to the conclusion that the defendant LLC "Google" is not the operator of the Google search system, as it does not administer the Google service, and therefore does not have access to Google's service and technical ability to somehow influence the information, placed on the Internet, including deleting the search engine of links to the website, indexed by the search service "Web search".

25 Translation proposed by Article 19, see supra note 13, p. 11.

26 See supra notes 23 and 24.

27 On this opinion: Тарасов Дмитрий, "Право на забвение в российском и европейском законодательстве", *Lex Digital Blog*, 29 Марта 2016, http://lexdigital.ru/2016/116/ (accessed on the 19/03/2015); Михайлов С.В., "Что такое право на забвение?" Журнал Суда по интеллектуальным правам , Сентябрь 2017, pp. 19-26.

28 Federal Law 149-FZ art. 10.3 point 8: "Оператор поисковой системы обязан не раскрывать информацию о факте обращения к нему заявителя с требованием, указанным в части 1 настоящей статьи, за исключением случаев, установленных федеральными законами" - "Research engine operators are obliged not to disclose information about the applicant's request made on the basis of the first paragraph of this article (the criteria), saved from the case prescribed by the Federal Law."

29 See supra note 16.

30 See supra note 13, p. 15.

THE RIGHT TO BE FORGOTTEN IN RUSSIA

and Yandex removed 172 links to pages referring to its notorious past, especially its implication in a criminal network. The applicant explains further that such information was inaccurate, as he has not been finally sentenced by a jurisdiction for such facts.[31] In any case, whether he is a public figure, has not been discussed.

More problematically is the case of the NGO Sova, committed to promote research and communication on radicalism and respect of human rights in Russia, which received notification from Google of a delisting of URLs relating to its website. In accordance with the Bill, this notification did not indicate either the authors' requests, or delisted URLs. The concerned information actually appeared to be about the trial of a neo-nazi group, which notably released online their beatings against minorities. On the 15th of August 2016, Sova sued Google before the Moscow arbitration Court on the ground of the right to access information as set in Article 29 of the Constitution of the Russian Federation as well as in Articles 3 and 8 of the Federal Law on Information 149-FZ. The case was brought on the same grounds before the courts of appeal and of cassation. Both concluded that the right to access information was not violated due to the very fact that such information is still available online. They somewhat expressed the need to underline that these webpages were accessible through other key words on the same research engine. More importantly, they excluded any review of the Bill with regard to the freedom of expression and to the general interest in information.[32]

III- CONCLUSION

In conclusion, a brief overview of the right to be forgotten in Russia demonstrates that its elaboration differs from that suggested by the CJEU. The criteria set by the legislator were translated in such a way as to offer maximal discretion to Internet users, but their effects are as much unforeseeable as they can actually provide such a right due to the lack of any equilibrium with fundamental rights. This blurs the Bill's *ratio legis* and, thus, the effect of terms employed. As operators are not bound to look for a balance between the privacy of users and the right to information nor the right of third parties, they can prevent delisting all along the proceeding on the very same criteria that were set by the legislator[33].

However, the broader context should be remembered. Legislator's shortcomings with regard to fundamental rights enshrined into the Constitution and International Conventions tie judges' hands when examining these cases. Although criteria set by the legislator do not bind operators to a framed legal test and in practice evidence to be shown may discourage applicants to the proceeding, operators did not release, for a long time, any statistic on the matter. Furthermore, even though operators can dismiss claims due to an indefinite scope, that also gives leeway for holding operators liable for their supposed negligence, which may moreover be subject to significant fines.

Finally, an expeditious adoption of this Bill - a month; extensive criteria leaning to the side of the users' discretion and an undefined operator's liability denote from the legislator a keen interest to enact literally the right to be forgotten

31 Иван Осипов, Бизнесмен Сергей Михайлов попросил удалить 172 ссылки о солнцевской ОПГ, Технологии и Медиа, РБК, 29 июня 2016, https://www.rbc.ru/technology_and_media/29/06/2016/5772528a9a7947eb45f57e9d (Accessed on the 18/03/2018).

32 Постановление от 12 сентября 2017 г. по делу № А40-205329/2016, Девятый арбитражный апелляционный суд, Москва (Statement of the 9th arbitration Court of appeal, 12/09/2017, in the case No. 40-205329/2016, Moscow); Постановление от 21 декабря 2017 г. по делу № А40-205329/2016, Арбитражный суд Московского округа, (Statement of the Arbitration Court of Moscow – i.e. cassation – 21/12/2017 in the case No.40-205329/2016).

33 See on similar conclusions: Николай Костенко, Права человека в Российской Федерации : сборник докладов о событиях 2015, Московская Хельсинкая Группа, 2016, с. 282.

LE DROIT A L'OUBLI AU CANADA : L'AFFAIRE GLOBE24H ET LE ROLE DU JUGE DANS LES REQUETES DE DEREFERENCEMENT

par Pierre-Luc Deziel
Professeur adjoint à la Faculté de droit de l'Université Laval, au Québec.

Cet article entend expliquer comment une décision récente de la Cour fédérale du Canada, l'affaire Globe24.com, avance une piste de solution intéressante et novatrice aux problèmes qu'engendre, sur le plan de la protection de la vie privée, l'indexation de certains sites Web. Cette solution serait de faire des tribunaux canadiens des "adjuvants" aux personnes qui souhaitent soumettre une demande de déréférencement auprès de moteurs de recherche comme Google, et ce, par le biais de jugements déclaratoires affirmant qu'un site contrevient aux lois de protection des données personnelles canadiennes.

Au Canada, il n'y a pas de droit à l'oubli tel que consacré en Europe par le Règlement général sur la protection des données (RGPD)[1] . Par le biais du droit d'accès aux renseignements personnels et l'obligation des entreprises à tenir des données qui soient à jour, la Loi sur la protection des renseignements personnels et les documents électroniques[2] (LRPDE) confère certes aux personnes un droit à la rectification des données personnelles, mais elle n'établit pas un droit au déréférencement tel qu'entériné par l'article 17 du RGPD. Comme le souligne la juge Desbiens dans C.L. c. BCF Avocats d'affaires:

> "[l]e droit d'une personne de faire rectifier dans un dossier qui la concerne des renseignements inexacts, incomplets ou équivoques n'est pas de l'ordre du «droit à l'oubli» qui vise à effacer des informations des espaces publics. D'ailleurs, il n'est pas certain que ce droit, reconnu en Europe, trouve application au Québec." (nous soulignons)[3]

L'incertitude évoquée par la juge Desbiens relativement à l'application d'un droit à l'oubli au Canada résulte en partie du fait que, bien que la loi canadienne n'établisse pas un droit explicite au déréférencement, les tribunaux supérieurs canadiens semblent, eux, présentement affairés à apporter une réponse plus claire, et peut-être plus positive, à cette question. Par exemple, dans *A.T c. Globe24h.com* [4], une décision de 2017, la Cour fédérale du Canada semble avoir identifié une piste de solution au problème que pose le référencement de pages Web contenant des renseignements personnels qui, bien qu'exacts et à jour, entraînent néanmoins certains préjudices aux personnes. Cette piste de solution serait de faire des tribunaux canadiens des adjuvants aux personnes qui souhaitent soumettre une demande de déréférencement auprès de moteurs de recherche comme Google. Selon la Cour fédérale, un jugement déclaratoire affirmant qu'un site Web contrevient aux lois de protection des données personnelles pourrait aider à persuader l'opérateur du moteur de recherches de procéder au déréférencement demandé[5] . Aux dires de la Cour, cette solution se présente peut-être comme "le moyen le plus pratique et efficace d'atténuer le préjudice causé à des personnes"[6] . Afin de bien saisir le

1 Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
2 Loi sur la protection des renseignements personnels et les documents électroniques LC 2000. c-5. Voir le principe 4.6 sur l'exactitude des renseignements personnels et le principe 4.9 sur l'accès aux renseignements personnels que l'on trouve à l'annexe A de la Loi.
3 C.L. c. BCF Avocats d'affaires, 2016 QCCAI 114
4 A.T. c. Globe24h.com, 2017 CF 114. Disponible en ligne: https://www.canlii.org/fr/ca/cfpi/doc/2017/2017cf114/2017cf114.html
5 Il convient peut-être de préciser que le jugement déclaratoire tranche également le litige, en ce sens qu'il affirme que le défendeur contrevient à la LRPDE.
6 Ibid, para 88

raisonnement de la Cour dans *Globe24h*, il convient de brièvement revenir sur les faits de cette affaire.

Le site web Globe24h.com est hébergé sur un serveur se trouvant en Roumanie. Le site republie des décisions de tribunaux canadiens que l'on peut trouver sur certains sites Web canadiens comme CanLII.org. Toutefois, contrairement aux décisions qui se trouvent sur ces sites, celles publiées par Globe24h sont indexées par des moteurs de recherche tiers comme Google[7] . Ainsi, en effectuant une recherche sur Google avec le nom d'une personne, il est possible d'avoir accès aux décisions de justice où ce nom apparaît. Le Commissariat à la protection de la vie privée du Canada (CPVP) a reçu 38 plaintes de personnes à l'endroit de Globe24h, et l'affaire fut portée devant la Cour fédérale. Les plaignants évoquent, notamment, que les décisions répertoriées par Globe24h comportent des renseignements personnels de nature délicate et que leur indexation par Google représente une atteinte à la vie privée engendrant de la détresse et de l'embarras.

Dans ses motifs, le juge Mosley a conclu que la LRPDE a une portée extraterritoriale et peut s'appliquer à Globe24h. S'appuyant sur la décision *SOCAN* de la Cour suprême du Canada[8] , le juge affirme que la Loi s'applique "dans toutes les circonstances où il existe *un lien réel et important* avec le Canada"[9] . Puisque Globe24h republie des décisions canadiennes trouvées sur des sites Web canadiens, et que les répercussions négatives de cette republication sont ressenties par des Canadiens et des Canadiennes, il existe un lien réel et important avec le Canada. Par conséquent, la LRPDE s'applique à Globe24h. Après avoir conclu que les actions du site Web contreviennent à la Loi, le juge Mosley s'intéresse à la question des réparations que la Cour peut accorder, une question qui touche à une problématique centrale du droit au déréférencement, c'est-à-dire sa mise en oeuvre.

Les tribunaux canadiens peuvent, certes, rendre des ordonnances extraterritoriales. Toutefois, ils demeurent réticents à rendre des ordonnances qui ne seront pas appliquées et qui ne produiront, par conséquent, pas ou peu d'effets[10] . Ainsi, dans *Globe24h*, la Cour souhaite d'abord évaluer la possibilité que les ordonnances qu'elle songe rendre produisent des effets positifs pour les plaignants. Bien que le juge semble initialement dubitatif quant à la "force exécutoire de toute ordonnance émise contre le défendeur"[11] , il prononce néanmoins un jugement déclaratoire précisant que les activités de Globe24h contreviennent à la LRPDE, ainsi que deux ordonnances correctives; la première en dommage-intérêts et la seconde demandant au site Web de retirer toutes les décisions canadiennes de ses pages.

Selon le juge, les ordonnances auront des effets concrets en ce sens qu'elles pourront certainement aider le demandeur à poursuivre ses recours en Roumanie[12] . Toutefois, il appert que ce serait le jugement déclaratoire qui pourrait avoir les effets les plus importants, notamment parce qu'il pourrait faciliter le processus de déréférencement que le demandeur pourra entamer auprès de Google. Dans un passage particulièrement intéressant, le juge Mosley souligne que:

> "Un jugement déclaratoire voulant que le défendeur a contrevenu à la LPRPDE, combinée à une ordonnance de mesure corrective, permettrait au demandeur ainsi qu'à d'autres plaignants de soumettre une requête à Google ou à d'autres exploitants de moteurs de recherche pour faire retirer de leurs résultats de recherche les hyperliens vers des décisions affichées sur le site Globe24h.com. Google est le principal moteur de recherche concerné, et ses politiques permettent aux utilisateurs de soumettre leur requête dans les cas où un tribunal a déclaré que le contenu d'un site Web est illégal. Il convient de noter que la politique de Google sur les annonces légales énonce que le fait de remplir et de soumettre le formulaire Google en ligne ne garantit pas qu'une quelconque mesure sera prise comme suite à la demande. Néanmoins, une telle requête demeure une voie qui s'offre au demandeur et à d'autres personnes touchées d'une façon similaire. Le CPVP [le Commissariat à la protection de la vie privée du Canada] considère que cette voie peut être le moyen le plus pratique et efficace d'atténuer le préjudice

7 La publication en linge des décisions judiciaires canadiennes relève du principe d'ouverture et de transparence des processus législatifs et judiciaires, un principe qui revêt une importance capitale dans les sociétés démocratiques. Toutefois, les sites web publiant ces décisions ne permettent généralement pas l'indexation par des moteurs de recherches externes. Cette politique a comme objectif de " minimiser les impacts négatifs de cette transparence sur la vie privée des participants aux affaires donnant lieu aux décisions judiciaires". Voir, par exemple, les politiques de protection de la vie privée de CanLii. En ligne: https://www.canlii.org/fr/info/vie_privee.html
8 Société canadienne des auteurs, compositeurs et éditeurs de musique c. Bell Canada, [2012] 2 RCS 326
9 A.T. c. Globe24h.com, 2017 CF 114, para 50.
10 Ibid, para 80-81.
11 Ibid, para 85.
12 Ibidem.

LE DROIT À L'OUBLI AU CANADA

> causé à des personnes, étant donné que le défendeur réside en Roumaine et ne dispose pas d'actifs connus."[13] (nous soulignons)

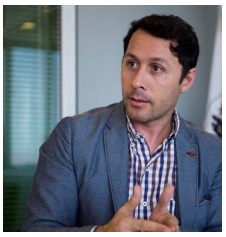
Ainsi, la voie du jugement déclaratoire représente, selon le juge et le CPVP, un moyen commode de répondre aux problèmes que peut engendrer, sur le plan de la protection de la vie privée, le référencement de pages Web par des moteurs de recherche. Or, on aura cependant compris que la décision rendue par la Cour fédérale dans *Globe24h* ne consacre pas explicitement un droit à l'oubli. En fait, le mot oubli n'apparait pas dans les motifs du juge Mosley. Néanmoins, cette affaire semble s'intéresser à des problèmes que l'on peut considérer comme relevant du droit à l'oubli, et répondre à certaines des difficultés que soulève la mise en oeuvre de ce droit.

Dans *Globe24h*, les pages indexées contiennent des renseignements personnels qui sont exacts et véridiques, mais qui, malgré tout, génèrent une détresse et de l'embarras pour les personnes qui en sont la source. De plus, ces renseignements sont publics et peuvent être trouvés ailleurs sur Internet, par exemple, sur les sites juridiques canadiens. La seule différence entre ces sites et Globe24h est le fait que celui-ci est indexé par Google. Le coeur de l'affaire porte donc sur cette idée de référencement par un moteur de recherche comme Google. Toutefois, Globe24h ne se solde pas par une ordonnance obligeant Google, ou tous autres moteurs de recherche, à déréférencer les pages du site Globe24h. Elle ne consacre pas plus un droit à l'oubli que pourraient faire valoir les citoyens et citoyennes canadiens face à Google. Elle opte pour une voie plus modérée, mais qui, si on se fie aux difficultés auxquelles se heurte la mise en oeuvre du droit au déréférencement établi par l'article 17 du RGPD, est peut-être plus réaliste, plus pratique et plus efficace. Cette voie est celle de fournir un argument supplémentaire aux personnes qui déposent une requête à Google pour que certaines des pages où leurs renseignements personnels apparaissent soient déréférencées. Cet argument prend la forme d'un jugement déclaratoire montrant que le contenu de la page Web en question contrevient à la LRPDE.

Évidemment, cette stratégie n'est pas sans soulever certaines difficultés. Est-ce fournir aux personnes des arguments face à Google est un rôle qui revient aux tribunaux? Cette stratégie ne risque-t-elle pas d'alourdir les requêtes de déréférencement? Puisqu'il existe des raisons de croire que ces demandes ne feront qu'augmenter, n'entrouvre-t-on pas ici la porte à une surcharge de tribunaux déjà embourbés? Ces questions devront certainement, elles aussi, trouver des réponses claires. Pour conclure, je me contenterai de mentionner que la décision rendue par la Cour fédérale dans Globe24h a produit des effets concrets et bénéfiques: le site globe24h.com n'existe aujourd'hui plus.

13 Ibid, para 88.

THE RIGHT TO BE FORGOTTEN IN ARGENTINA



By Juan Gustavo Corvalán
Deputy Attorney General in Contentious, Administrative and Tax Matters of the Public Prosecutor´s Office of the Autonomous City of Buenos Aires.

To this date, Argentina lacks a legal platform to address whether or not Internet intermediaries are responsible for the content available within their network and the role of the "right to be forgotten" within this framework. This has created a legal gap that has generated an uneven atmosphere, which can be exemplified through the various precedents within the current legal history of the country. Through the Supreme Court's decision in the Rodriguez case, which establishes that research engines (Internet intermediaries) are not responsible for the content that they upload to their networks, it was understood that there was no sanction required for the intervention that these engines provide in legal situations where there are rights being affected. It is argued that due to the nature of the activity, which corresponds strictly to the provision of information - independently of its content- no attribution of responsibility for the damages should be enforced since it exceeds their operations; excluding situations where the damage has been properly informed and not been addressed.

The digital revolution[1] and the denominated Fourth Industrial Revolution,[2] are modifying radically the world we live in. In this context of change, privacy and the control of our information on the Internet are issues of primary importance for constitutional States: who can access certain personal information? How is that information used? How is it stored? Or, for how long? The answers to these questions outline serious challenges to the judicial practitioners.[3]

In this scenario, the debate on the effectiveness of the "right to be forgotten" arises. This debate, in synthesis, can be approached from a double perspective: on the one hand, as a right to "give back" to the individual the control over their personal information; on the other hand, to give the individual the possibility to "free its past from a rigid digital mould." [4]

To approach the content and scope given to this right in Argentina, we shall develop the following three aspects:

First: briefly analyze the conceptualization of the right to be forgotten, from the terms established in the precedent "*Google Spain*"[5] of the Court of Justice of the European Union (hereinafter, "CJEU.")

Second: synthesize the judicial precedents in the Argentine law, specially focusing on the "Rodriguez" case of the Supreme Court of Justice of the Argentine Republic (hereinafter, "CSJN," for its syllables in Spanish, or "Supreme Court"), considering it a leading case on the matter.

Third: outline the bills presented in the National Congress and how these intend to regulate the responsibility of the intermediaries and the right to be forgotten. Here, the attention is focused on the relevant matters of the

1 ECLAC (United Nations Economic Commission for Latin America and the Caribbean), "The new Digital Revolution: from a consumption Internet to a production Internet," August 2016, Economic studies, The Digital Revolution, Institute of Economic Studies, 2016.
2 See Schwab, Klaus, "*The forth Industrial Revolution*", Ed. Debate, 2016; and also, Word Economic Forum, "Living the Fourth Industrial Revolution", available at: https://www.weforum.org/es/agenda/archive/fourth-industrial-revolution/
3 Report from Frank La Rue - former special reporter from the UN for the Promotion and Protection of the Rights of Opinion and Expression - pages 5/6.

4 CELE (Freedom of Expression Centre of Study), "*The Right to be forgotten: between data protection, memory and personal life in the digital era*", Palermo University, page 3.
5 Court of Justice of the European Union, "*Google Spain, S.L., Google Inc. v/ Agencia Española de Protección de Datos (AEPD), Mario Costeja González*", ruling from May 13th, 2014. Available at: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

THE RIGHT TO BE FORGOTTEN IN ARGENTINA

bill that received preliminary approval in the National Senate.

I-PRELIMINARY CONSIDERATIONS.

It is important to start outlining some conceptual distinctions, by answering the following two questions:

A-What are the Internet intermediaries and under which ways can its liability be established?

All Internet communications are obtained by intermediaries. "Internet intermediaries" is a broad term that refers to the entities that allow individuals to connect to the Internet and share content. There are different types of intermediaries, such as internet access suppliers, web hosting service suppliers, social network platforms and search engines. There is a distinction between internet intermediaries and "content producers". The later are people or organizations in charge of producing information and posting it online.[6]

On this aspect, there exist four models or types of liability that can be attributed to the intermediaries regarding online information:[7]

i) Absolute immunity: in this model, intermediaries are not responsible for any kind of illegal content published or shared by individuals through their service.

ii) Objective liability: here, the intermediaries will always be responsible for the content users express through them, regardless of their knowledge on said content. The only way intermediaries can exempt their liability will be to constantly monitor and/or filter or block content potentially considered illicit and/or that might compromise their liability.

iii) Conditioned immunity: the intermediaries shall not be responsible if certain conditions or requirements are satisfied. The intermediaries are offered a "safe port": that is to say, as long as they comply with certain specific duties, they shall not be responsible for illegal content from third parties. Here, at least two variants or systems can be perceived: a) notice and takedown, that requires the user to consider that certain content is illegal and to notify the intermediaries so as to filter the content, b) notice and notice, the user notifies the intermediaries of the existence of illegal content, and they shall notify that to those who generated the content.

iv) Subjective liability: in this model, the behavior of the intermediaries will be analyzed, so as to determine whether all the precautions have been considered or if there has been negligence.

B-What is meant by "search engines" and "thumbnails"?

The name given to "search engines" is related to the service they supply of searching automatically content on the Internet that is related to or characterized by a few search words determined by the user. They work as a technical tool that favors access to the desired content by automatic references.[8]

On the other hand, the term "thumbnails" refers to the link of an original image uploaded to a website, hinting to the user the content of the website, and also allowing the user to decide whether to access the page or not.[9]

II-RIGHT TO BE FORGOTTEN. TERMINOLOGICAL ISSUES.

The right to be forgotten usually includes the right to change, evolve and contradict oneself. Fundamentally, it is based on the principle of the limited extent of data retention that was established by the National Commission on Informatics and Liberty in France.[10] In essence, the abovementioned principle determines that information cannot be archived in digital files indefinitely, but for the necessary time so as to comply with the proposed objective for which it was collected.[11]

6 Defense on freedom of expression and information, "*Internet intermediaries: Dilemma on responsibility – Q&A Sessions*", available at https://www.article19.org/fr/resources/internet-intermediaries-dilemma-liability-q/

7 Meléndez Juarbe, Hiram A., "Intermediaries and Freedom of Expression", in Bertoni, Eduardo Andrés (comp), "*Towards an Internet free of censorship*." Proposed for Latin-American, Buenos Aires, Palermo University, 2012, pages 116/117.

8 Conf. Thibault Verbiest, Gerald Spindler, Giovanni M. Ríccio, Aurélie Van der Perre, "*Study on the Liability of Internet Intermediaries*", November 2007, page 86 and whereas 14° of ruling "Rodríguez".

9 Autonomous entity in charge of protecting data processing in that country.

10 According to the definition of the Supreme Court of Justice of the Argentine Republic on the judgment "Rodríguez María Belén v/ Google Inc. on damages," October 28, 2014, whereas 19° and 20°.

11 CELE, "*The Right to be forgotten: between data protection, memory and personal life in the digital era*", Palermo University, page 16 and Commission Nationale de L'Informatique et Des Libertés, "Rapport d'activité 2011", available at http://www.ladocumentationfrancaise.fr/rapports-publics/124000334/index.shtml

THE RIGHT TO BE FORGOTTEN IN ARGENTINA

Regardless of the several names[12] given to it, the right to be forgotten essentially involves the decision of "erasing" content of the search engines whenever it is against privacy or the free exercise of fundamental rights.

This concept, even though it is not new[13], is supported by the recognition of the right to be forgotten established by the CJEU by making the intermediaries responsible for the data contained in their search engines[14]. Therefore, according to the ruling, an individual can request that certain personal information be removed from the results of search engines, provided that: a) the personal information was inadequate, not pertinent, out of date or excessive, in that it is not related to the purpose for which it was uploaded in a first place, and b) that there is no public interest.[15]

However, it is important to consider that the conception and development of the right to be forgotten is related to the historical and cultural context of certain countries.

For example, during the 20th century, Argentina suffered systematic and massive violations of human rights, due to the interruption of democratic governments, as of military and/or civic coups; indeed, the last civic and military dictatorship (1976/1983) caused the perpetration of multiple crimes against humanity. In this context, the right to be forgotten can be considered as a grievance, if those individuals involved in the violation of human rights could request Google to make that information impossible to find.[16]

Thus, this matter, among others, determines that the right to freedom of expression shall prevail over the right to be forgotten. Or, in other words, different nuances can be detected to perceive if the perspective is focused on the protection of personal data, or if it focused on the freedom of expression. In both scenarios, the following questions arise regarding substantive aspects: shall the individuals have the power to suppress veridical information on their past? If so, what are the limits that shall be established by law? But, also, a question of procedural character arises: if the right to be forgotten exists, who shall be in charge of its application and under what rules?

In the case exposed below, we will be able to observe how the Argentine Supreme Court of Justice approached these matters and, basically, the current contrast with the European judicial precedents regarding the requirement of a court order to remove content from the Internet.[17]

III-ARGENTINE JUDICIAL PRECEDENTS.

As anticipated, Argentina lacks a rule that regulates in a specific way the liability of intermediaries. Factually, this represents a difficulty that can be evidenced in the judicial precedents analyzed below:

A-The Supreme Court perspective.

The Supreme Court of Justice of the Argentine Republic's "Rodriguez" case can be summarized as follows:

i. The case facts. The case dates from 2006 when the model María Belén Rodriguez filed a complaint against Google Inc.[18] since, when typing her name on the search engine, she was related to web pages with erotic and/or pornographic content.

At first instance the complaint was sustained by considering that the search engines have been culpably negligent by failing to absolutely block or impede the existence of injurious or illegal content which might cause damage to the plaintiff's personal rights. Then,

12 As affirmed by Fleischer, the right to be forgotten is usually represented as from the well know Rorschach test, to which individuals assign several meanings. See Fleischer, Peter, "The right to be forgotten, or how to edit your history," in his persona blog, January, 2012, available at http://peterfleischer.blogspot.com.ar/2012/01/right-to-be-forgotten-or-how-to-edit.html

13 The origin of the right to be forgotten can be found in the concept of Frech Law droit à l'oubli and from Italian Law diritto all'oblio, which, in general, "can be perceived as the «right to silent events from the past that are not longer taking place »". Ferrari Verónica – Schnidrig Daniela, "*Intermediaries Liability and the Right to be forgotten*." Contributions for argentine lesgislative discussions, CELE, June 2015, page 9. It can also be related with German laws elaborated so as to assist rehabilitated criminals, see Keller, Daphne, "*The Right to be forgotten, from Europe to Latin America*," at Del Campo, Agustina, "*Towards an Internet free of Censorship II. Latin America Perspectives*," CELE, Palermo University, 2017, page 174.

14 CJEU, "The representative of an Internet search engine is responsible for the treatment applied to personal data that appear in websites published by third parties," press release nº70/14, May 14, 2014. Available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf

15 Whereas 81 y 94.

16 The current director of the Argentine Agency on the Protection of Data affirms that in such sense, it will be an *"insult for our History (so as to put it in a soft way)*," Bertoni, Eduardo, "The Right to be Forgotten: insult for the Latin American History, The Huffington Post, September 24, 2014, available at https://www.huffingtonpost.com/eduardo-bertoni/the-right-to-be-forgotten_b_5870664.html

17 Keller, Daphne, "*The Right to be forgotten, from Europe to Latin-American*," at Del Campo, Agustina, "*Towards an Internet free of Censorship II. Latin America Perspectives*," CELE, Palermo University, 2017, page 184.

18 Afterwards she amended the complaint against Yahoo from Argentina S.R.L (Argentine Limited Liability Company).

THE RIGHT TO BE FORGOTTEN IN ARGENTINA

ordered Google and Yahoo to pay a fine and to definitely delete all the links between her name, image and photos and sites and activities with erotic content. The judgment was appealed by all parties. The National Court of Appeals with jurisdiction on Civil matters partially revoked it by dismissing the claim against Yahoo and accepting the one against Google; reduced the latter's compensation; and eliminated the transcriptions, conforming it to the subjective liability regime. Both the plaintiff and Google filed extraordinary appeals, which were granted, against this judgment.

ii. The Court decision.[19] Having previously held a public hearing,[20] the CSJN ordered that the search engines shall not be held responsible for the content that they upload to the network. As a principle, the Court established that the search engines shall not be held responsible for content they have not created, since this situation would be comparable to punishing the libraries for having catalogued books that have injurious content, alleging they have "encouraged" the damage.[21]

The judgment's argumentative approaches can be summarized as follows: 1) The subjective civil liability might be assigned to search engines when the content, which is accessed through them, damages rights, and 2) The mechanism to establish subjective liability on search engines requires that they be notified of damage to the right to privacy, honor and/or image, and that they failed to act assiduously or omitted to block the access to that information.

Regarding the first approach, even if the plaintiff wanted the case to be judged according to the objective liability rules, the CSJN will discard the application of these rules and apply the subjective liability ones considering that:

A) "Browsers" are not obliged to "monitor" (supervise or control) the content that is uploaded to the network and are provided by each web page responsible;

B) As a corollary to this logic, the absence of monitoring obligation is followed by the absence of liability;

C) If an illegal activity is being carried out – which, by hypothesis, shall be punished - those responsible for the path that leads to the place where it is being performed cannot be punished, stating that it had eased the access to it.

On this basis, the Court concluded that the search engines are initially not responsible for the content that they have not created; that is to say, according to CSJN, search engines connect web sites but are not responsible for its content. Thus, the Court considered that establishing an objective liability regime shall lead to the discouragement of the existence of search engines, which have an essential role in the right to search, receive and spread information and opinions freely on the internet.[22]

In relation to the second approach, -proceedings to establish the subjective liability-the CSJN noted that there are some cases where the search engines shall be liable for external content; that is whenever it has effective knowledge of the content's illegality. On this sense, and as obiter dictum, the judgment established the "effective knowledge required for subjective liability". Under such requirement, the Court questioned, in light of the lack of legal regulation, whether it is enough for the injured party to give private notice to the "search engine" or if, on the contrary, it is mandatory that the notification be made by a competent authority. Considering this, two (2) situations were distinguished: a) cases where the damage is evident and coarse, b) cases where the damage is debatable, dubious and needs to be proven.

The first set of cases correspond to "illegality of injurious content", where the illegal nature -civil or criminal- of the content is evident and directly results by accessing the page identified by the damaged party in a reliable notification or, depending on the case, of any party, without the need to further assessment or clarification. On the contrary, the second set of cases correspond to those cases where the injurious content eventually damages the honor -or other types of damages-, but such damages need to be established in a judicial or administrative forum for its effective determination.[23]

In the case of the latter it was concluded that it is appropriate to require a notification by a competent judicial or administrative body; the simple private communication by the party that is considered damaged is not enough, and even less that by an interested party.[24]

Lastly, the Court pronounced a ruling on the thumbnail stating that they are not judged for the responsibility that might be held on an internet page - by the wrongful publishing or circulation of images - but for being the intermediary whose only role is to link to this information. Consequently, it stated that:

19 The majority decision was made by Carlos Fayt, Eugenio Zaffaroni and Elena I. Highton de Nolasco. Currently, the latter is the only one occupying the position at the Supreme Court
20 Open court held on May 21st and 29th, 2014. Available at: https://www.youtube.com/watch?v=Bxlikawvc-I
21 Whereas clause 19° of Lorenzetti and Maqueda's vote.
22 Whereas clause 19° of Lorenzetti and Maqueda's vote. It is not appropriate to apply different rules to the "search by image" and the "text search" applications, as both link content which have not been created by them
23 Whereas clause 18°.
24 Whereas clause 18°.

THE RIGHT TO BE FORGOTTEN IN ARGENTINA

1. It is not appropriate to apply different rules to the "search by image" and the "text search" applications, as both link content which have not been created by them;[25]

2. It is appropriate to confer liabilities to the web page creator and not to the search engine and its results,[26] and

3. The search engines might be held liable if, once they have been properly notified of the violation, they do not act with due diligence[27] .

This last statement shall be appropriate whenever, to ensure a balance of interests, the links associated with the person and the damage they cause are precisely identified. Under these terms, the protection provided is a type of subsequent indemnification that prevents all generalization, which shall affect the flow of thoughts, messages or images and consequently the freedom of expression.[28]

iii. The dissidence on the judgment. The judgment has a partial dissidence of two members[29] of the Supreme Court who believed that:

a) The model shall be indemnified for the use of her image due to the "lack of consent" on its publishing;

b) The Court should proceed to a writ of injunction aiming to delete existent links, whereas it is oriented to delete other existent links so as to avoid the future connections with the same characteristics.[30]

With relation to the first matter they agreed that a) on Argentine law it is unavoidable to resort to Act 11,723 on Intellectual Property which states that it is mandatory to have the consent of the owner of the personal right for the publishing of his image, b) the legislator, as a norm, prohibited the image reproduction, which it only relinquishes if certain circumstances relating to general interest suggests they should prevail.

As per the second aspect, they agreed that the search engines' activity on the internet is not incompatible with the civil liability regime on its preventive aspect, in case of actual threat of damage, to prevent the repetitive spreading of detrimental information on the plaintiff personal rights. This conclusion is based on the general principle of damage prevention that states that all individuals have the duty to avoid causing unjustified damage[31] and to adopt reasonable measures to prevent it from happening or to diminish its scope.[32]

In subsequent cases, the Argentine Supreme Court has referred to this precedent to rule on the merits and issue a judgment.[33]

B-Other precedents by lower courts

Previous to the judgment in the "Rodriguez" case, the Argentine judiciary had to deal with similar situations; however, due to the lack of legal regime and judicial precedents from the Supreme Court, there were not uniform judicial responses. Hereinafter there are some examples of different responses that were given.

In the case "Bluvol",[34] an entrepreneur brought a lawsuit against Google for the existence of a blog with his name. The two courts that heard the case applied different responsibility regimes. In the lower court, the complaint was sustained by applying the objective liability regime, ruling that the search engines shall give compensation to the plaintiff. In the upper court, the objective liability regime was dismissed, arguing that Google, as an intermediary, shall not automatically be liable for third parties' illegal actions, as it is impossible to previously assess all the information that is spread. Even though the upper court ruled that Google was liable, it did so by applying the subjective liability regime, stating that the search engine behavior was analyzed and considered negligent.

In the case "Carrozo "[35] Google and Yahoo were ordered to compensate a model for the use of her image on

25 Whereas clause 20°.
26 Whereas clause 20°.
27 Whereas clause 22°.
28 Whereas clause 31° of Lorenzetti and Maqueda's vote.
29 Judges Lorenzetti and Maqueda.
30 Whereas clause 31° of Lorenzetti and Maqueda's vote.
31 They determined few origin requirements and characters of the preventive prohibition aiming to avoid repetition, aggravation or damage persistence, namely: i. Criteria with less restriction possible shall be analyzed, and the most appropriate mean to guaranty the proportionality and efficiency for the aim fulfillment, ii. The affected or threatened party shall provide, according to the case circumstances, the identification rules necessary for its creation, iii. The abovementioned preventive protection is independent from the recessionary one; iv. It works independently from a new effective configuration of damage to the objective and subjective rights of an individual, as the mere existence of foreseeable threat to the protected legal right enables its legal origin. See whereas clauses 33 and 34.
32 Whereas clause 31° of Lorenzetti and Maqueda's vote.
33 CSJN, «*Da Cunha, Virginia v. Yahoo de Argentina S.R.L and other on damages*» and «*Lorenzo, Bárbara v. Google Inc on damages*», judgements passed on December 30th 2014.
34 National Court of Appeals with jurisdiction on Civil matters, "*Bluvol Carlos v. Google Inc. and others for damages*", judgement passed on 05 December 2012
35 National Court of Appeals with jurisdiction on Civil matters, "*Carrozo Evangelina v. Yahoo de Argentina and others for damages*", judgment passed on 10 December 2013.

pornographic sites by the application of the objective liability regime. In this case the court considered the search engines were acting hazardously and that made them automatically liable for the damage they caused.

In another similar case, "Da Cunha"[36] on the contrary, a subjective liability regime was applied holding the search engine liable as it was notified and did not remove the content.

IV-TOWARDS A REGULATORY POLICY: A REVISION OF SEVERAL BILLS.

With the exponential growth of Internet and Big Data, new challenges arise that need to be solved in order to ensure users' rights. On this sense, Argentina lacks rules that regulate these matters. However, the following regulatory documents can be consulted:

i. Act 26,032: As it establishes that "the search, reception and spread of information and ideas of all kinds, through Internet service, are considered within the constitutional guaranty that protects the freedom of expression"[37] .

ii. The new Civil and Commercial Code of the Argentine Republic[38] : Establishes an objective liability regime (sections 1722 and 1723) and a subjective liability regime (section 1724).

iii. The Manila Principles: These determine that: a) intermediaries shall be protected by law from liability for third parties' content; b) content restriction without an order issued by a judicial authority shall not be required; c) requests for content restriction shall be clear, unmistakable and shall respect the due process; d) law, orders and content restriction practices shall comply with the necessity and proportionality assessments and the due process; e) transparency and information of actions taken shall be within normative policies and practices on content restriction.[39]

Since 2006, there are bills that have not been considered. Particularly, on the Argentine Republic's Senate there are some proposals that try to consider, within a generic scope for internet regulation, intermediaries or search engines' responsibility.

During the last period, there were two bills pending treatment: bill S-942/2016[40] and bill S-1865/2015. Towards the end of last year, a bill that unifies the aforementioned bills had been partially passed by the Argentine Republic's Senate.

This bill aims to regulate the internet service providers' responsibility, ensuring the freedom of expression and the right to information taking into consideration the preservation of the rights of honor, privacy, and image.

As an exception, it holds responsible the internet service providers with subjective liability with exemption from liability to monitor and supervise content generated by third parties.[41] In that way, it disposes a search engine to be responsible for the external content when, having been notified of the illegality, it did not act as instructed by the judge.

As it can be noted, the legal mechanism chosen was the determination of "effective knowledge", establishing that "in no case shall be considered that the self-regulation system implies effective knowledge"[42] Likewise, taking into consideration the Supreme Court's doctrine on the judgment aforementioned, it ascertains that the complainant shall precisely identify the link where the content in question is located or the proceedings for its access.[43]

It is important to mention that this bill focuses on the Argentine internet provider's responsibility but does not specifically regulate the right to be forgotten. It also has other omissions: a) it does not regulate violations of intellectual property rights, b) it is not on the same wavelength as the duty of not damaging and damage prevention established in section 1710 of the Argentine Republic's Civil and Commercial Code, and c) it omits the creation of a protocol for notification and rapid deletion of illegal or injurious content that the CSJN classified with special care.

On the other hand, and with relation to this, there is another bill S-444/2015[44]- that focuses on a regulation that warrants that all individuals shall exercise their right of suppression contemplated on section 16 of Act 25,326 - protection of personal information-, of certain

36 National Court of Appeals with jurisdiction on Civil matters, "*D.C. V. v. Yahoo de Argentina S.R.L and others for damages*", judgment passed on 10 August 2010. This case reached the Supreme Court and the extraordinary remedy entered was dismissed.
37 See section 1° of Act 26,032.
38 The term "new" is used as it was enforced in August 2015.
39 Manila principles on intermediaries' responsibility. Guideline for best practices that determine the content intermediaries' responsibility on the promotion of freedom of expression and innovation. March 24, 2015.
40 The bill has been approved on the Senate and sent to the lower chamber for its revision together with bill S-1865-2015.
41 See bill's sections 4° and 5°.
42 See bill's section 7°.
43 See bill's section 6°.
44 Text available at: http://www.senado.gov.ar/parlamentario/comisiones/verExp/444.15/S/PL

THE RIGHT TO BE FORGOTTEN IN ARGENTINA

indexed-linked content by the search engines resulting from a search under an individual's name.

There were other bills on the Argentine Republic´s Senate. Among them, it is worth mentioning, even though it is no longer in the docket[45] - bill 1918/14.[46] This bill established that companies providing internet services to final users have the duty to install filters that shall block the access to the list of restricted access sites determined by the National Communications Commission.

V-BRIEF FINAL CONSIDERATIONS.

The right to express oneself through the Internet encourages the freedom of expression from an individual dimension as well as from a collective dimension. Through the Internet, the personal right each individual has to make public, transmit, share and exteriorize ideas, opinions, beliefs, criticisms, among others is exercised. As from the collective dimension, the Internet constitutes an instrument to guarantee the information's liberty and the formation of public opinion.

Nevertheless, when we refer to the right to be forgotten, figures behind this issue are significant. Intermediaries receive many fake requests to remove data. In the context of the "right to be forgotten", Google revealed that it received 1.6 million requests to remove websites, and that almost 57% of the requests did not represent a valid judicial claim in agreement with the Law on the Right to be Forgotten passed by the European Union.[47]

In this context, and different to what the CJEU did, the Argentine Supreme Court gave the judicial authorities the power to decide whether to remove the information.[48] Also, it is related to previous judicial precedents of the Argentine Supreme Court regarding the protection of freedom of expression; according to the Supreme Court, in a democratic regime, press freedom represents one of the liberties, to the extent that, without its due protection, there would be a deteriorated democracy or a purely nominal one.[49]

In the end, every restriction, sanction or limitation to the freedom of expression in Argentina shall be subject to a "restrictive interpretation".[50] Therefore, we are of the opinion that the judicial precedent of the Supreme Court has been inclined preponderantly to the application of the mentioned liabilities due to the abuses caused during their exercise, by the commission of crime or illicit civil acts.[51] The Rodriguez judgment is aligned to this.

Finally, as supported by several authors, it is believed that it is important that Argentina moves forward in the legislation on this matter[52] , such as other countries of the region, like Brazil[53] , Chile[54] and the United States of America.[55]

Also, the re-interpretation of Section 13.3 of the American Convention on Human Rights shall be considered in relation to this issue. This provision states that "right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions".[56]

In conclusion, to copy the European scheme, at least in totum, does not seem a suitable idea. On the contrary, the historical and current context of human rights in Latin America shall be considered, mainly in what refers to freedom of expression and its compatibility with the right to be forgotten.

45 Expired in February 2016 and has been filed.
46 Text available at http://www.senado.gov.ar/parlamentario/comisiones/verExp/1918.14/S/PL
47 Keller, Daphne, "*The right to be forgotten: from Europe to Latin America*", in Del Campo, Agustina: "*Towards an Internet free of censorship II. Perspectives in Latin America*", CELE, University of Palermo, 2017, page 181.
48 An important critic to the judgment "Google Spain" is that it effectively delegated the decisions that balance the intimacy and freedom of expressions right of the users "in the hands of foreign technological companies; instead of delegating said liability in national courts". Keller, Daphne, "*The right to be forgotten: from Europe to Latin America*", in Del Campo, Agustina: "*Towards an Internet free of censorship II. Perspectives in Latin America*", CELE, University of Palermo, 2017, page 188.
49 Judgements: 331:1530, among others.
50 Judgements 316:1623.
51 Judgements: 119:231; 155:57; 167:121; 269:189; 310:508, among many others.
52 Tomeo, Fernando, "2012 goes away with technology but without law"" and "The right to be forgotten in the web is forgotten" available at: https://www.lanacion.com.ar/1531755-el-derecho-al-olvido-en-la-web-paso-al-olvido; Pucinelli, Oscar, "*The right to be forgotten in the right of Data protection. The argentine case*," in Revista Internacional de Protección de Datos Personales, N°1, December 2012; Cárrega Alberto F., "Partial approval for the bill unifying liability of internet services providers", available at: goo.gl/JaJPLt
53 Act N°12,965 (Civil framework of the internet,) April, 2014.
54 Act 17,336, amended by Act N°20,345, on May, 2010.
55 Section 230 of Communication Decency Act. Without prejudice of application, according to the case, of the Digital Millenium Copyrights Act, year 1198.
56 American Convention on Human Rights, article 13.3

LE DROIT À L'OUBLI DANS LE DROIT BRÉSILIEN

par Rafael Valim
Professor of Administrative Law and Foundations of Public Law at the Catholic University of São Paulo – PUC/SP

par SIlvio Luis Ferreira Da Rocha
Professor of Administrative Law and Civil Law at the Catholic University of São Paulo – PUC/SP

En droit brésilien le droit à l`oubli n'est pas véritablement consacré ni par la loi, ni par la jurisprudence. Il existe néanmoins des précédents dans lesquels on reconnaît à une personne impliquée dans le cadre d`une procédure pénale, le droit de ne pas se voir rappelé des faits dépréciatifs, après un certain temps écoulé. Si la jurisprudence brésilienne se réfère à l'affaire *Google Spain*, elle considère que l`on ne peut pas imposer à un tiers – qui n`est pas le propriétaire de l`information que l`on veut voir oubliée – la fonction de retirer l'accès au grand public d'un ensemble de données déterminé. Il n'existe donc pas une obligation de désindexation de certaines informations pour les moteurs de recherche. Il nous semble que cette appréciation soit erronée, puisque, dans l'état technique actuel c`est parfaitement possible, une fois organisée la recherche, d`exclure des résultats pouvant associer la personne à une information.

Malgré l'importance du droit à l'oubli dans notre société de l'information, la discussion sur le droit à l'oubli n'est pas arrivée à maturité au Brésil. La doctrine est encore en développement et, bien qu'il existe déjà plusieurs décisions de justice, la Cour suprême n'a pas statué sur la question.

En outre, il n'y a pas de loi spécifique sur le droit à l'oubli. Il n'y a que quelques projets de loi en cours[1] , mais ces derniers ne sont que le résultat de problèmes conjoncturels, sans un nécessaire débat public.

Dans ce contexte, cet article vise à exposer la position majoritaire de la doctrine sur le droit à l'oubli et à offrir une analyse critique des décisions judiciaires importantes sur ce sujet.

I-DROITS FONDAMENTAUX DE LA COMMUNICATION

Actuellement, dans la société de l'information vivement marquée par le développement exceptionnel des médias de communication, il est reconnu, à la faveur de la personne humaine, un ensemble de droits concernant toutes formes d'expression ou de réception d'informations, connu comme les « droits fondamentaux de la communication ». D'après Valerio de Oliveira Mazzuoli, ils « intègrent l'axe fondamental de la conception contemporaine des droits de l'homme qui s'expriment de façon multifonctionnelle et qui permettraient plus ou moins l'expression communicative. Ces droits résulteraient de la somme des droits ou libertés suivants: (a) la liberté d'expression *stricto sensu*; (b) la liberté d'opinion; (c) la liberté d'information; (d) la liberté de religion; (e) la liberté de recherche scientifique; (f) la liberté de création artistique; (g) la liberté d'édition; (h) la liberté de journalisme; (i) la liberté de presse; (j) la liberté de radiodiffusion; (k) la liberté de programmation; (l) la liberté de télécommunications; et (m) et la liberté de navigation dans les milieux numériques.[2] »

Tous ces droits, vus dans leur ensemble, formeraient une « mosaïque communicative », nouvelle catégorie de droits formés à partir des droits individuellement considérés, comme ayant pour finalité de renforcer et de garantir globalement l'accès de toutes les personnes aux moyens de communication et d'expression (individuels et collectifs) actuellement existant, lesquels résulteraient en des « droits fondamentaux de la communication» (*Kommunikationsgrundrechte*) des citoyens. [3]

L'exercice de ces droits fondamentaux de la communication peut, toutefois, contraster avec d'autres

1 http://www.internetlab.org.br/pt/opiniao/5especial-direito-ao-esquecimento-no-congresso-nacional/

2 Direitos Comunicativos como Direitos Humanos: Abrangência, Limites, Acesso à Internet e Direito ao Esquecimento, publié in Revista dos Tribunais, vol. 960/2015, p. 249.

3 Direitos Comunicativos como Direitos Humanos: Abrangência, Limites, Acesso à Internet e Direito ao Esquecimento, publié in Revista dos Tribunais, vol. 960/2015, p. 249.

LE DROIT À L'OUBLI DANS LE DROIT BRÉSILIEN

droits fondamentaux. Ainsi surgit le débat salutaire autour de la possibilité que ces droits puissent souffrir des restrictions, en particulier s'ils sont confrontés à d'autres droits fondamentaux, tels que (a) l'honneur ou la réputation des autres personnes, (b) la protection de la sécurité nationale, de l'ordre public, ou de la santé ou de la morale publique ; (c) l'intimité ; et (d) la possibilité de réinsertion sociale. Se construit alors une nouvelle doctrine au sujet de la constitution d'un autre droit fondamental, de même importance, dénommé le droit à l'oubli.

II-LE DROIT À L'OUBLI

Le droit à l'oubli, traduction de l'expression "right to be forgotten", également nommé par l'expression "*right to be let alone*" aurait son origine dans l'étude de la tutelle de l'intimité. Le droit à l'oubli s'est également développé dans le domaine pénal. A ce titre, l'article 202 de la Loi d'Exécution Pénale prévoit expressément la non-disponibilité de certaines informations processuelles, une fois la peine exécutée ou révoquée (Loi 7.210/84). Ainsi, certains faits ayant eu lieu dans le passé devraient être oubliés et ne plus être évoqués.

Pour certains, au Brésil, le fondement du droit à l'oubli serait le principe de la dignité de la personne humaine, prévu à l'art. 1er, III, de la Constitution Fédérale brésilienne. Le champ d'application du droit à l'oubli serait d'empêcher que soient préservés, dans la mémoire collective, des faits et des informations qui puissent porter atteinte à l'honneur, à la bonne réputation de l'individu, après un délai raisonnable, ou, encore, parce que le souvenir de ces faits lui provoquerait des dommages moraux. Normalement, l'oubli de ces faits se fait par l'écoulement du temps. Il se trouve néanmoins que la technologie a actuellement permis la construction d'outils qui sont capables de stocker pendant un temps très long toutes ces informations. De cette façon, il n'est plus possible d'ignorer l'impact que la technologie peut causer à la personne, notamment à l'aide d'un outil de recherche qui se montre capable de réunir, en quelques secondes, toute une gamme d'informations dûment structurées sur une personne donnée, et qui ne sont pas toujours souhaitables.

Donc, ce qui est finalement recherché lors de l'invocation du droit à l'oubli, c'est de retirer ou de supprimer une information déterminée ou le contenu d'un lieu déterminé, tel qu'un magazine ou URL (*Uniform Resource Locator*), de promouvoir la désindexation de certains mots clefs de sites déterminés, lorsqu'une recherche est réalisée chez un fournisseur Internet spécifique, ou, encore, de marquer l'adresse d'une page Web pour qu'elle ne figure plus dans les résultats d'un moteur de recherche déterminé, si une recherche sur un certain thème est réalisée. Cela signifie que, lorsqu'un internaute tapera sur le clavier le contenu recherché dans un champ de recherche, même si la page est encore publique, elle ne sera pas exhibée de façon directe sur la liste des résultats. [4]

Ainsi, la meilleure façon de définir le droit à l'oubli serait de le considérer comme un droit autonome de la personnalité, à l'aide duquel l'individu peut exiger l'exclusion d'informations à son sujet lorsqu'un laps de temps suffisant s'est écoulé, pour rendre une telle information inaccessible, en observant la nécessité d'exercer un équilibre entre les droits d'accès à l'information et le droit aux libertés d'expression, scientifique, artistique, littéraire et journalistique.

En résumé, le droit à l'oubli comprendrait le droit d'oublier et le droit d'être oublié. Il pourrait être relié à d'autres droits de la personnalité, tels que l'intimité, l'honneur, l'image ou une autodétermination informative spécifique. Ce droit à l'autodétermination informative correspondrait à la faculté reconnue à la personne de gérer et de disposer du contenu des informations qui circulent à son sujet, en particulier sur Internet, si ces informations sont exclusivement privées. Ce droit lui permettrait d'oublier le passé et de réécrire un nouveau futur. Pensons, par exemple, à une actrice qui s'est distinguée dans des films pornographiques ou érotiques, mais qui, s'étant convertie religieusement, aimerait oublier le passé et ne pas permettre l'accès à ce dernier.

C'est pourquoi, lors de la VIème Journée de Droit civil du Conseil de la Justice Fédérale, a été approuvée la Déclaration 531, selon laquelle le droit à l'oubli doit être reconnu au sein de la tutelle de la dignité de la personne humaine dans la société de l'information.

La Cour Supérieure de Justice, en particulier le Quatrième et le Sixième Tribunal de cette Cour, se sont également, à plusieurs reprises, prononcés en faveur du droit à l'oubli, ainsi que le révèlent les jugements HC 256.210/SP, Sixième Tribunal, rendu le 03/12/2013[5] ; RESp 1335153/

4 Chiara Spadaccini de Teffé, O direito ao esquecimento: uma expressão possível do direito à privacidade, *Revista de Direito do Consumidor*, vol. 105/206, pp.33-64, p. 39.
5 https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201202111500&dt_publicacao=13/12/2013

LE DROIT À L'OUBLI DANS LE DROIT BRÉSILIEN

RJ, Quatrième Tribunal rendu le 28/05/2013[6] et RESp 1334097/RJ, Quatrième Tribunal, rendu le 28/05/2013[7] .

Dans ces jugements, ainsi que nous le verrons ci-après, le droit à l'oubli a été défini comme le « droit de ne pas être mentionné contre sa propre volonté, spécifiquement en ce qui concerne des faits dépréciatifs, de nature criminelle, dans lesquels on a été mêlé, mais par la suite innocenté ». Considérant les effets juridiques de l'écoulement du temps, pour les choses jugées mentionnées, il a été évalué que le Droit stabilise le passé et confère une prévisibilité au futur à l'aide de différentes règles (prescription, déchéance, pardon, amnistie, non-rétroactivité de la loi, respect au droit acquis, acte juridique parfait et chose jugée).

A-Dimensions du droit à l'oubli

Le droit à l'oubli couvre différentes situations.

La première, qui a été à l'origine de sa consolidation par la jurisprudence, concerne *l'historique des antécédents processuels criminels.* Le droit à l'oubli assure que seront oubliés et dissimulés les procès et les condamnations pénales antérieures, une fois la peine remplie et le condamné réhabilité pour empêcher des situations discriminatoires se rapportant à l'obtention d'un travail par exemple. Même dans ce cas, cependant, le droit à l'oubli ne sera pas appliqué lorsque les faits passés sont en rapport à des faits historiques ou concernent une personne exerçant une activité publique ou considérée comme une figure publique, ou encore, lorsque la personne essaie de s'appuyer sur son passé pour démontrer son innocence ou une grave injustice. Cette exception reflète le droit de la société de préserver sa mémoire collective ; la seconde se réfère à l'intérêt public d'avoir accès à toutes les circonstances concernant l'exercice de la fonction publique ; la troisième se place aux côtés de ceux qui cherchent à prouver leur innocence et récupérer, dans la mesure du possible, l'honneur et l'image contre des attaques commises à leur encontre.

La seconde dimension possible du droit à l'oubli renvoie à l'ensemble significatif d'informations personnelles qui permettent l'identification d'une personne. Ces informations peuvent être collectées, réunies et conservées avec le consentement préalable de la personne. La collecte de ces informations est à la charge des bases de données publiques ou privées. Aussi, ces informations sont fréquemment mises à disposition de façon indue pour un usage commercial, tel que l'envoi de publicité ou de *mails*, même s'il existe, sur ces informations, un devoir de confidentialité et de non divulgation à des tiers. Empêcher l'utilisation indue des données personnelles ne requiert pas nécessairement le recours au droit à l'oubli. Il peut tout simplement s'agir d'un cas clair et explicite d'utilisation abusive. Le droit à l'oubli exige, quant à lui, qu'un laps de temps se soit écoulé pour pouvoir être activé.

La troisième dimension probable du droit à l'oubli est la mémoire du passé, qui accumule les erreurs et les mésententes de la personne et qui, exposée indistinctement, pourrait lui causer des préjudices.

La quatrième dimension possible au droit à l'oubli est la plus sensible de toutes, étant donné qu'elle concerne la circulation des informations sur *internet* et, surtout, car il existe en elle une prédisposition à éterniser les informations, dans la mesure où elle compte, comme nous l'avons vu ci-dessus, sur un système de recherches efficace et avec un réseau d'ordinateurs interconnecté qui permet de copier et reproduire ces informations dans différents pays.

III-PRÉCÉDENTS JUDICIAIRES SUR LE DROIT À L'OUBLI

A-Resp. 1.334.097/RJ : Le droit à l'oubli dans la civilisation du spectacle

Dans le *Resp. 1.334.097/RJ* étaient discutés l'exposition de l'image et le nom d'un individu qui avait été accusé d'être le co-auteur d'une série d'homicides ayant eu lieu le 23.07.1993, dans la ville de Rio de Janeiro, la « Tuerie de Candelária ». Dans un reportage diffusé en juin 2006, lors d'un épisode du programme de télévision *Linha Direta-Justiça,* il a été désigné comme l'un des individus impliqués dans la tuerie, bien qu'il ait été absout pour déni de participation par l'unanimité des membres du Conseil de Sentence du Tribunal du Jury.

Abordée par la chaine de télévision, l'individu s'est refusé à donner une interview et a démontré son manque d'intérêt de voir son image accolée à un tel fait dépréciatif. Il a allégué que le programme offrait au public un fait déjà passé, qui avait incité à la haine sociale dans la communauté où il vivait, portant préjudice à son droit à la paix, à l'anonymat et à la vie privée, et portant même préjudice aux droits de sa famille, pour avoir indument été associé à l'image d'un tueur. Il a, en outre, fait valoir que cela avait porté préjudice à sa vie professionnelle et sociale et l'avait mené à se défaire de ses biens et partir de la communauté où il vivait pour des raisons tenant à sa sécurité et de celle de sa famille. Le résultat a été

6 https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201100574280&dt_publicacao=10/09/2013
7 https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201201449107&dt_publicacao=10/09/2013

LE DROIT À L'OUBLI DANS LE DROIT BRÉSILIEN

la condamnation de la chaine de télévision, en seconde instance, au paiement de la valeur de 50.000,00 BRL.

En appel, la chaine de télévision a soutenu l'absence de fondement pour l'obligation d'indemnisation en raison de l'absence de l'illicéité. Selon elle, il n'y avait pas eu d'offense à la vie privée, à l'intimité de l'auteur car les faits diffusés étaient publics. En outre, elle invoquait que le droit à l'oubli ne pouvait empêcher le droit d'informer. Le Tribunal a toutefois considéré que les droits de la personnalité étaient liés à la dignité de la personne humaine et, dans le conflit avec ceux-ci, l'adoption de paramètres de proportionnalité et de modération légitimerait l'atténuation de l'une des valeurs constitutionnelles en collision. Cette préférence pour la dignité de la personne humaine est prévue aux articles 1er, III et à 5ème, IX, de la Constitution Fédérale brésilienne, et aux articles 11, 20 et 21 du Code Civil brésilien. L'historicité du crime et l'intérêt public ne peuvent pas empêcher la reconnaissance du droit à l'oubli, car celui-ci pourrait « signifier un correctif – tardif, mais possible – des vicissitudes du passé, soit d'enquêtes policières ou de procès judiciaires pyrotechniques et injustes, soit de l'exploitation populiste des médias ». Pour le rapporteur, il y aurait dans la loi brésilienne plusieurs normes qui affirmeraient le droit à l'oubli telles que : (i) la prescription ; (ii) le délai maximum pour l'inscription d'informations négatives du consommateur dans des bases de données (art. 43, § 1er, du Code de Défense du Consommateur); (iii) la réhabilitation criminelle (art. 93 du Code Pénal et art. 748 du Code de Procédure Pénale) et ; (iv) le secret du casier judiciaire une fois la peine accomplie (art. 202 de la Loi des Exécutions Pénales).

Pour lui, la liberté d'informer ne serait pas un droit absolu et illimité mais un droit limité par la vraisemblance de l'information, par l'existence d'intérêt public et par l'intervalle temporel pour définir la licéité de la divulgation. Ainsi, dans les procès criminels, la reconnaissance du droit à l'oubli représenterait l'évolution humanitaire et culturelle d'une société, ainsi que la concrétisation de la loi, en garantissant l'espoir de réhabilitation de la personne humaine. En résumé, la « Tuerie de la Candelária » serait un évènement historique, apte à être divulgué, mais sans mention du nom et sans l'utilisation de l'image de l'auteur.

Dans cette affaire, la Cour Supérieure de Justice a décidé de reconnaître le droit à l'oubli comme découlant de la dignité de la personne humaine et des droits de la personnalité (vie privée, intimité, honneur et image). La *ratio decidendi* de ce précédent établit que la personne concernée par un procès criminel a le droit de ne pas être rattachée à ce fait dépréciatif après l'écoulement d'un certain temps. Etant personnage public ou pas, elle a le droit d'être oubliée et l'atteinte à ce droit suscite le devoir d'indemnisation pour les dommages moraux provoqués.

B-Resp 1.316.921/RJ – Xuxa versus Google : Le droit à l'oubli dans la société de l'information

Il s'agit d'un appel spécial interjeté par Google Brasil Internet Ltda. contre la décision de la Cour d'appel de Rio de Janeiro, dans laquelle Maria da Graça Xuxa Meneghel, célèbre présentatrice de programmes de télévision pour le jeune public, a obtenu un succès partiel provisoire dans une action judiciaire visant à obliger la société à retirer de son site Web de recherches nommé "Google Search", les résultats relatifs à la recherche par l'expression « xuxa pédophile », ou encore, tout autre résultat qui puisse associer le nom de l'auteure, écrit partiellement ou intégralement, et indépendamment de la graphie, qu'elle soit correcte ou fausse, à une quelconque pratique criminelle.

Pour le rapporteur considère que, nonobstant l'existence indiscutable de relation de consommation dans le service rendu par les sites de recherches *via* internet, leur responsabilité doit être restreinte à la nature de l'activité qu'ils développent, correspondant à la fourniture de recherche, visant à faciliter la localisation d'informations sur le Web. En ce qui concerne le filtrage du contenu des recherches faites par chaque usager, il ne s'agirait pas d'activité intrinsèque au service rendu, et donc on ne pourrait pas considérer comme défectueux le service rendu par le site Internet qui n'exercerait pas ce contrôle sur les résultats des recherches. En outre, pour le rapporteur, il faut considérer que les moteurs de recherche réalisent leurs recherches au sein d'un univers virtuel, dont l'accès est public et non restreint, c'est-à-dire que son rôle se limite à l'identification de pages du web dans lesquelles se trouve une certaine donnée ou information, même illicite mais qui sont librement véhiculées. Par conséquent, selon lui, l'action devrait se retourner non pas contre les moteurs de recherche, mais contre les sites WEB ou les fournisseurs de contenu. Même la quantité de pages destinées à l'exploitation de contenu illicite ne saurait justifier le transfert au simple fournisseur de service de recherche de la responsabilité, de l'identification de ces sites. Le rapporteur a d'ailleurs souligné que cette forme de censure entraverait la localisation de toute page Internet avec le mot ou l'expression interdite, indépendamment du caractère légal ou non de son contenu, ce qui ce qui empêcherait le droit à l'information.

Cette affaire n'a pas été jugée de façon définitive. La Cour d'appel de Rio de Janeiro, dans une décision du 4 mai

LE DROIT À L'OUBLI DANS LE DROIT BRÉSILIEN

2017[8], a, pour autant, adopté la même position que celle de la Cour Supérieure de Justice : il n'y a pas d'obligation de désindexation pour les moteurs de recherche.

C-AgInt. dans le Resp. nº 1.593.873-SP

Il s'agit d'un appel interjeté dans le cadre d'une action d'injonction, jugée par *S.M.S.* à l'encontre de Google Brasil Internet Ltda., par laquelle il avait demandé et obtenu le blocus définitif de recherches en son nom, ces dernières pouvant mener à des pages Internet reproduisant des images de nudité.

Le rapporteur, dans son vote, a, d'une part, cité des précédents de la Cour Supérieure de Justice, qui ont reconnu le droit à l'oubli tout en soumettant chaque situation spécifique à une évaluation. Il a, d'autre part, souligné que le cas soumis à son appréciation porte sur des fournisseurs de recherche qui ne détenaient pas proprement l'information que l'on désirait voir oubliée. Aussi tout en mentionnant une décision de la CJUE favorable à l'oubli (CJUE, 13 mai 2014, *Google Spain, Google Inc. et l'Agence Espagnole de Protection de Données et Mario Costeja Gonzales*), il observe que la décision part d'hypothèses légales très distinctes, en particulier une absence de loi générale sur la protection de données personnelles des citoyens brésiliens. Pour lui, le Cadre Civil de l'Internet (Loi nº 12.965/2014) n'a pas établi une protection générale des données personnelles ; la protection prévue à l'article 7, alinéa X, serait restreinte aux informations fournies par le propre individu à un fournisseur d'applications d'Internet déterminé. De surcroît, l'Internet fondé sur le Cadre Civil de l'Internet constitue, d'après le rapporteur, un ensemble de protocoles logiques, structuré à l'échelle mondiale pour l'usage public et sans restriction, dont la finalité est de permettre la communication des données entre terminaux à l'aide de différents réseaux intégrés par de nombreux sujets qui offrent différents types de services et utilités. Ils mentionnent là les fournisseurs de *backbone* (épine dorsale) qui détiennent la structure de réseau capable de traiter de grands volumes d'information et qui assurent la connectivité de l'Internet ; les fournisseurs d'accès qui acquièrent l'infrastructure des fournisseurs de *backbone* et la revendent aux usagers finaux ; les fournisseurs d'hébergement qui stockent les données des tiers et leurs concèdent un accès à distance ; les fournisseurs d'information qui produisent les informations divulguées par le Web et les fournisseurs de contenu, qui mettent à disposition sur le réseau les données créées ou développées par les fournisseurs d'information ou par les usagers du Web eux-mêmes. Il considère, en outre, que les moteurs de recherche sont une espèce de fournisseurs de contenu, et n'incluent pas, n'hébergent pas, n'organisent pas ou ne gèrent pas les pages virtuelles indiquées sur les résultats mis à disposition ; les moteurs de recherche se limitent à indiquer les adresses où peuvent être trouvés les termes ou expressions de recherches fournis par l'usager. Le rapporteur a également réaffirmé que la responsabilité des moteurs de recherche doit être limitée à la nature de l'activité qu'ils développent et a alors répété les arguments présentés *Resp 1.316.921/RJ – Xuxa versus Google*. Par conséquent, étant donné que le demandeur ne stocke pas les informations que la défenderesse prétendait exclure des résultats des recherches réalisées avec son nom, il ne pouvait pas figurer comme partie au procès. Finalement, le Cadre Civil de l'Internet ne fonde, pour le rapporteur, que partiellement un droit à l'oubli, vu que son article 7 I. et X, prévoit la prérogative du particulier de demander, indépendamment de toute justification, l'exclusion de ces données personnelles qu'il aurait lui-même fournies au fournisseur de l'application d'Internet. Selon lui, la législation mentionnée ci-dessus ne permet pas d'imputer à un tiers qui ne détient pas l'information que l'on veut voir oubliée de remplir la fonction de retirer l'accès d'un ensemble déterminé de données au public en général.

IV-QUELQUES REMARQUES CRITIQUES DE LA JURISPRUDENCE BRÉSILIENNE

Le positionnement adopté par la Cour Supérieure de Justice dans la décision *Resp. nº 1.593.873-SP* nous semble mal fondé. La personnalité est la base de l'attribution d'une série de droits qui seraient propres et innés à la personne humaine : les droits de la personnalité. La personnalité serait l'ensemble de caractères propres de la personne. Ces caractères sont passibles de défense juridique s'ils sont violés. D'où le jugement selon lequel les « droits de la personnalité sont les droits subjectifs de la personne de défendre ce qui lui est propre, c'est-à-dire, l'identité, la liberté, la sociabilité, la réputation, l'honneur, la production/création intellectuelle.[9] »

L'idée des droits de la personnalité a été développée à partir de la révision de la conception que les biens et les intérêts protégés par l'ordre juridique, sont uniquement des choses, des personnes et des produits de l'invention sur lesquels l'individu exerce sa propriété.[10] La datation

8 http://www1.tjrj.jus.br/gedcacheweb/default.aspx?UZIP=1&GEDID=000464418ACE030ED63B527CAF48D0DB41A3C50626305033&USER=

9 Gofredo Telles, Direito subjetivo – I, in Enciclopédia Saraiva do Direito, v. 28, p. 315.

10 D'après Gilberto Haddad Jabur, in 'Liberdade de Pensamento e Direito à vida Privada', p.32 : « l'idée – revue par Andréas von

LE DROIT À L'OUBLI DANS LE DROIT BRÉSILIEN

de la reconnaissance de cette catégorie de droits est impossible. Nous savons simplement qu'elle a gagné en importance avec l'École de Droit Naturel et son ensemble de droits innés, considérés préexistants et immédiats à la naissance de la personne. Elle a, de surcroît, obtenu un renfort considérable avec la Déclaration des Droits de l'Homme et du Citoyen de 1789. Les droits de la personnalité ont également profité de l'inclusion du principe de la dignité humaine dans les textes des Constitutions. L'inclusion de ce principe a, en effet, donné aux droits de la personnalité une dimension évaluative. Ce sont eux qui concrétisent le principe de la dignité de la personne humaine. Les Constitutions ont, par ailleurs, commencé à prévoir dans leurs textes une protection spécifique aux droits de la personnalité. Citons, à titre d'exemple, la Constitution brésilienne qui, en son article 5, X, protège la vie, la liberté, l'intimité, la vie privée, l'honneur et l'image. Ce n'est que maintenant, avec la promulgation du nouveau Code Civil, que cette constitutionnalisation de certains droits de la personnalité a eu une systématisation adéquate au sein du Droit Privé.

La circonstance que le droit à l'oubli et celui à l'autodétermination informative constituent des droits de la personnalité justifierait déjà la concession d'une protection exceptionnelle, en particulier lorsqu'ils sont en confrontation avec une activité entrepreneuriale à but lucratif, indépendamment de la législation spécifique. Une des fonctions des Droits Fondamentaux et de Droits de la Personnalité est d'inhiber, d'empêcher des comportements qui puissent se révéler nocifs. En d'autres termes, dans le cas en question, il ne s'agit pas d'inhiber les moteurs de recherche pour l'élimination de termes, d'expressions et de paroles, de façon à avoir une exclusion a priori de toute information, mais, simplement, une fois la recherche organisée, d'exclure les résultats pouvant associer la personne à cette information, ce qui, dans l'état technique actuel, est parfaitement possible.

Il s'agit, en dernière analyse, d'appliquer également au Brésil, l'orientation décidée par la CJUE dans le sens que: I) Un fournisseur d'application de recherches doit être considéré responsable des données personnelles qu'il traite; II) La responsabilité existe, même si le serveur de données du fournisseur de l'application de moteur de recherches se trouve hors du territoire européen; III) Les exigences légales une fois remplies, le fournisseur de l'application de moteur de recherches se voit obligé de supprimer la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, les connexions à d'autres pages publiées par des tiers et qui contiennent des informations sur cette personne, même lorsque leur publication dans les pages en question est, en soi, licite.

Tuhr – que les biens et les intérêts que protège l'ordre juridique, ne sont pas uniquement des choses, des personnes et des produits de l'invention, sur lesquels l'individu exerce sa propriété, mais aussi, et au premier plan, la propre personne, le propre sujet à qui l'usage intellectuel et corporel sont destinés tous les droits auxquels on vient de se référer, s'est solidifiée et a donné origine à ce que l'on peut surnommer de *droits subjectifs de la personnalité* ».

THE RIGHT TO BE FORGOTTEN IN CHILE. DOCTRINE AND JURISPRUDENCE.

By Pedro Anguita Ramírez
Professor, School of Communication
Universidad de los Andes, Chile.

The threats to the fundamental rights that, for some years, have been generated by the Internet and the progressive increase of content that rises and stays in a perennial way in this network, has been distributed with some homogeneity to all the countries of the world whose population has an appreciable degree of connectivity. Chile has not been the exception. An increasing number of citizens have brought legal action before the courts of law against Google and social media that maintain their digital newspaper archives online. The article will expose both the doctrine and jurisprudence on the so-called right to be forgotten in Chile.

Google's unlimited storage capacity has gradually become a threat to the privacy of citizens around the world. The impact of Google has been so great in our lives that for a long time its name has become a verb. Googlear means to enter a name in the most used search engine worldwide to search certain content on the Internet. Whenever we do not have much time or imagination and we want to find some information, before we think about the corporate website of a state company, organization or entity, we use Google. Neither are there many occasions when we want to know the background of a person with whom we think to live, hire or simply know about, that we do not consult Google. The original idea of Google began as a doctoral thesis developed by the company's founders, Larry Page and Sergey Brin, who intended to constitute a search engine based on an algorithm that ordered web pages based on the number of visits that they receive. As usual, this unlimited Google storage capacity has gradually become a threat to the privacy of citizens around the world, since, like the person imagined by Jorge Luis Borges, author of *Funes el Memorioso,* Google does not forget and reminds us and everyone who wants to know something about our lives, that everything that once appeared in a medium of communication, a portal of any public or private institution, Facebook, or Blogs hosted on the Internet, is retained. It is difficult to imagine a life without Google, but as a technological breakthrough some threats to our fundamental rights arise. The lawsuits that have been instigated in Chile in order to eliminate content on the Internet have been presented, as we will see, against Google and also regarding media sites that have their editions and programs in their digital files available on the Internet.

I-THE RIGHT TO BE FORGOTTEN IN CHILE

The decision of the Court of Justice of the European Union, in the well-known case *Google Spain SL, Google Inc. v Spanish Data Protection Agency, Mario Costeja González,* C-131/12, issued in 2014, had effects in Chile and around the world. This ruling was cited by the first and only sentence pronounced by the Supreme Court of the country, that decided to apply the right to forget to a notice that appeared on Emol, the web portal of the company El Mercurio, in January 2016, in the case *Graziani vs. El Mercurio SAP*, as we will explain. Since 2012, protection actions have begun to be taken in Chile against Google, in order to de-index information that is located by the search engine. Although those affected by content on the Internet in Chile often invoke the ruling in the *Costeja* case, our courts do not yet fully notice the negative externalities they produce in relation to the fundamental rights of citizens, in many cases a flagrant violation, exempting Google of all responsibility. On the other hand, we should point out that, in Chile, almost without exception, the jurisprudence regarding the right to forget has been constituted by the interposition of constitutional actions called resource or action of protection. It is a precautionary, emergency procedure that fits very well

THE RIGHT TO BE FORGOTTEN IN CHILE

with the objectives of those affected, who promptly wish to eliminate or disindex links or URLs containing information or images that damage their right to honor and/or their right to their private life, guaranteed in our Political Constitution.[1] So there is an important difference with what happens in other countries, especially those that are part of the European Union, where its citizens use the principles, rights, actions and institutions contemplated in their respective laws of protection of personal data. In other Latin American countries such as Argentina, civil damages actions have been taken against intermediaries, such as Google and Yahoo, where it has demanded not only the suppression of content, but also the payment of large sums of money as reparation for the moral damage suffered by the owners of the data and images.[2] In Chile on the other hand, civil remedies have not been awarded for moral damages against search engines like Google.

II-THE LEGAL CONFLICT IN THE RIGHT TO FORGET

The affected rights that can be violated by the volumes of information that circulate indefinitely on the Internet and that the search engines like Google make possible to locate in a few seconds, are the right to the protection of personal data and the right to privacy and honor; the latter two protected by our Political Constitution and common and special legislation, both civil and criminal.[3] The activity of Google for its part, is protected by both the freedom to develop an economic and business activity, and by freedom of expression, specifically, freedom of information.[4] The traditional conflict between the right to honor and privacy and freedom of information is usually solved according to two criteria, namely, truthfulness and public interest in the first right. And only the public interest, regarding the right to privacy. Both criteria appear to be insufficient to resolve conflicts such as those caused by search engines such as Google. In the case of *Costeja*, and the actions that have been raised in Chile, it is difficult to justify an infringement of the right to privacy by the insertion ordered by the Social Security of Barcelona, since it is not appropriate to unduly interfere in any of the various areas protected by such a right. Neither does the right to privacy protect cases of persons who have been investigated for any wrongdoing, and less so if the courts have assigned responsibility for such acts. The inc. end of art. 30 of Law No. 19,733 lists a set of facts covered by the scope of the right to privacy, such as sexual, conjugal, family or domestic life, except, a qualified exception: that constituting a crime. So a person, who has been convicted of a sexual offense, and in general an offense of any kind, can not claim a violation of his private life by disclosing his identity.[5] Neither can they make a claim for injury to the right to honor, if they have been the subject of a criminal action and have been given responsibility, since the same article quoted, letter f)

1 The only action, by which it was acted by the ordinary way in summary judgment, was directed against La Estrella de Arica belonging to the company El Mercurio. An attorney requested to remove nineteen news URLs that had reported the print and digital version of that newspaper, about their arrest, formalization and conviction for a common crime. The trial ended in a transaction, in which the company that owns the newspaper, committed to eliminate nine URLs, also agreeing to require through Google, Yahoo and MSN the closure of access to the URLs that appear the news in their engines of searches. Millalonco with Company Agustín Edwards, 17th Civil Court of Santiago cause rol No. 27835-2012. Four years later the newspaper The Clinic published a journalistic article on the civil action that deduced Millalonco, reason why this plaintiff filed an appeal of protection against that means and Google. Case related to Millalonco Díaz, Juan with Google Inc.-Comercial The Clinic S.A.

2 On September 12, 2017, the Argentine Supreme Court (CSNJ) dismissed a civil action against Google Giambutas, Carolina Valeria v. Google Inc., confirming the thesis presented by that court in case Rodríguez, María Belén Google Inc. and Yahoo Argentina SA in October 2014. In both cases, the plaintiffs are professional models who claim to associate their images with pornographic and commercial sex sites carried out by search engines.

3 The common criminal protection protects the right to privacy essentially in art. 161-A of the Criminal Code and the right to honor in arts. 412 to 431 of the same legal text. The civil protection of the right to privacy is governed only by the general rules of noncontractual civil liability contained in TIT. XXXV of Book IV of the Civil Code. The civil protection of honor is also regulated by the general rules of the Civil Code., Law No. 19.733 on Freedom of Opinion, Information and Exercise of Journalism. This last law constitutes the special regulation of the criminal and civil responsibility derived from a violation to the right to the honor spread through means of social communication. Law No. 19.733 therefore does not regulate the criminal or civil protection of the violation of private life committed through a means of communication. Only the art. 30 refers to privacy.

4 The art. 19 of the Constitution: No. 12. The freedom to express opinions and to inform, without prior censorship, in any form and by any means, without prejudice to respond to crimes and abuses committed in the exercise of these freedoms (...). The N° 21, for its part, establishes the right to develop any economic activity that is not contrary to morality, public order or national security, respecting the legal regulations that govern it.

There is a qualified exception: the media can not reveal the identity of perpetrators, accomplices or concealers of an illegal act. The same prohibition exists in Chile with regard to victims of sexual crimes. Art. 33 of Law N° 19,733.

5 There is a qualified exception: the media can not reveal the identity of perpetrators, accomplices or concealers of an illegal act. The same prohibition exists in Chile with regard to victims of sexual crimes. Art. 33 of Law N° 19,733.

qualifies as in the public interest, the facts related to the commission of crimes or guilty participation. In the field of freedom of expression, and specifically freedom of information, the public interest, as we noted, was the relevant and common criterion in weighing the conflict between the right to honor and the right to privacy.

Finally, due to its uniqueness, some authors have argued that the right to be forgotten, exceeds levels of protection conferred by the right to privacy, honour and the rules on protection of personal data, finding as the best foundation, the free development of the personality, violated by being subject to interference that hampers the plan of life of those affected.[6] Our Political Constitution did not explicitly recognize the free right of the personality, although, during its elaboration, its inclusion was proposed,[7] which in the judgment of the Constitutional Court, *"... does not mean to ignore that the free development of the personality constitutes an expression of the dignity of all persons, which is emphatically affirmed in the first paragraph of Article 1 of the Fundamental Law"*.[8]

III-THE PRECEDENTS OF THE RIGHT TO BE FORGOTTEN

A-Criminal Record

Some areas of the right to be forgotten have an old existence in our legal system. This dimension relates firstly to those convicted of crimes, which are empowered to require the removal, or the omission of the criminal history from the extract of identification and criminal records.[9] The object is to make it possible for them to be reintegrated into society, to forget about the criminal acts they have committed, once their sentence has been served. For this purpose, there is a set of legal and regulatory rules that set requirements and conditions to erase the criminal record and/or the medical records of a person.[10] The right to a criminal offense, even protected in our country, in the Penal Code, which qualifies as one of the cases of serious injuries, imputation of a crime or simple crime punished or prescribed, in art. 417, No. 3.

B-The Protection of Personal Data

A second area associated with the right to be forgotten in Chile, whose first rule was issued in 1925, relates to limits on the communicability of commercial, financial or banking defaults by institutions that assess the solvency and risk of people. Thus, just as the legal system contemplates the neglect of crimes, in the

6 In Spain SIMON CASTELLANO has founded the right to oblivion in art. 10.1 of the Spanish Constitution, which states: «The dignity of the person, the inviolable rights inherent to it, the free development of personality, respect for the law and the rights of others are the foundation of the political and Social peace «. The right to free development of personality was enshrined in the German Fundamental Law of 1949, which is then incorporated in several Constitutions from the second half of the s. XX. Such a right enables fundamental rights not expressly recognized in constitutional or international texts to be considered as implicit rights. Thus, in cases where the right to oblivion is raised, courts of justice can resort to a broad right, such as the right to free development of personality, to integrate by means of rules of interpretation, principles, values and purposes and to provide protection To people affected, who do not have an explicit and specific right to the technological development generated by the Internet and Google.

7 See the debate in the Commission of Studies of the New Constitution in the judgment of the Constitutional Court Role No. 1638-2010, reasons Forty-fourth to Fiftieth.

8 Tribunal Constitutional, rol No. 1683-2010, Fifty-first argument. In the same sense, he had stated in STC Role No. 389-2003 that «respect for and protection of the dignity and rights to privacy of life and communications are an essential basis for the free development of the personality of each individual. Subject, as well as its manifestation in the community through the autonomous intermediary groups with which society is structured.» (Reason 21).

9 For the American jurist Jeffrey Rosen, the intellectual roots of the right to oblivion are found in French law - droit à l'oubli - held by criminals, who, having served their sentences, may oppose the publication of the facts of their conviction and imprisonment. This point constitutes in Rosen's opinion, one of the divergences between the United States and Europe, explaining that in his country the publications of criminal records are protected by the First Amendment, citing the case of two Germans who required Wikipedia to remove from their criminal records the murder of a famous actor. ROSEN, Jeffrey, The Right to Be Forgotten, 64 Stan. L. Rev. Online 88.

10 Our legal system has mechanisms to eliminate antecedents and also to require the omission of annotations in the registries of convicts. To eliminate the background, Supreme Decree No. 64, (1960), regulates the elimination of criminal records, annotations, and the granting of certificates of precedence, regulating the elimination of criminal records in the General Register of Convictions. Secondly, Law No. 19,962 (2004) provides for the elimination of certain medical records, authorizing the removal of the General Register of Convictions, in cases where the person concerned has been recognized in the Report of the National Commission on Political Prison and Torture. Regarding the omission of criminal annotations in certificates of antecedents, three norms are in force. In the first place, Law No. 18,126, (1983), establishes penalties that indicates as substitutive the private or restrictive sentences of Freedom, contains in its art. 29 the requirements for making the request. Secondly, Law No. 19.628 on Protection of Private Life, also entitled, on the Protection of Personal Data, (1999), contemplates in its art. 21 the conditions for requesting the omission of convictions for offenses, administrative infractions or disciplinary offenses, on the certificates of antecedents for private and special purposes. Finally, Decree Law No. 3482, (1980), grants pardons, reduces the penalty and eliminates book entries for persons convicted of crimes indicated, under the conditions it expresses, in its art. 9, contemplates four requirements to require the omission of criminal records.

economic field, there are also deadlines, which, after compliance, prevent these institutions from informing others about the non-fulfillment of certain obligations, and there is therefore a kind of right to forget about such breaches.[11] Since the issuance, in 1999, of Law No. 19,628, the protection of all personal data was extended in Chile, granting its owners, among others, the right of elimination, or cancellation and blocking, which relate to the right to forget, although such legislation has never been used. However, Law No. 19,628 expressly excluded from its competence the processing of personal data carried out in the exercise of freedom of opinion and information.[12] So, in our country, the activity developed by the media in traditional or electronic media are excluded from the scope of the law. For this reason, those interested in removing content that is disseminated through an information company on the Internet, can not base their claims on the provisions contained in Law No. 19,628. A related subject is linked to the qualification or definition of the work carried out by search engines like Google. If we consider that your activity is protected by the freedom of information, requests for deletion of content could not be based on infringement of the protection of personal data. Such issues, in any case, have not yet been addressed by our courts.

C-The Draft Laws on the Right to be Forgotten in the Chilean Legal System

Chilean law does not prescribe the right to be forgotten. Those affected by content circulating on the Internet, as we have noted, have raised constitutional actions, called protection resources, which require, in order to thrive, the accreditation of an arbitrary or illegal act that deprives, disturbs or threatens any of the rights or freedoms contained in art. 19 of the Constitution, among which are the two rights most closely linked to the right to forget; the right to privacy and the right to honor. The broad powers that the national courts have in this constitutional action allow them to order the withdrawal or suppression of content on the Internet - usual petitions of those affected. However, three bills related to the right to oblivion have been submitted. The first began its legislative process in the month following the issuance of the ruling of the CJEU in the *Costeja González* case, being its decisive influence. It proposed to incorporate a single article to Law No. 19,628 on the protection of personal data, enshrining the right of every person to demand from search engines or websites the ability to delete their personal data.[13] The second initiative links the right to oblivion to negative economic personal data, proposing that credit market players use this background for the purposes that were collected, provided they are current, specific and accurate, providing fines and civil solidarity against its non-compliance, prohibiting communication, as well as its use, treatment and transfer.[14] The third project suggested incorporating the right to forget in the law of personal data protection and considered that the search for information on the Internet constitutes a processing of personal data.[15] According to the progress of legal initiatives, there is no warning that in the near future they can become law.

IV-LEGAL ACTIONS AGAINST GOOGLE

As we argued, only legal actions have been brought against Google, probably because it is, the search engine with a great reach, more popular not only in Chile, but in the vast majority of countries in the world.[16] The constitutional and precautionary action has been, with a qualified exception, the exclusive way of action to require Google to disinfect harmful or unwanted records. This apparently effective mechanism has been rarely used in Chile, although this number has grown progressively.

11 A critical analysis of the regulation of personal data protection in our country, and specifically the regulations on commercial, economic and financial data, see Chapter IV of our book *La Protección de Datos Personales y el Derecho a la Vida Privada*, ANGUITA RAMÍREZ, Pedro, (trans. The Protection of Personal Data and the Right to Privacy), Editorial Jurídica, Santiago, Chile, 2007, p. 367-476.

12 Art. 1, inc. 1, Law No. 19,628. The treatment of personal data in registers or data banks by public bodies or individuals shall be subject to the provisions of this law, except in the exercise of the freedom to express opinions and inform, which is Shall be regulated by the law referred to in article 19, No. 12, of the Constitution. The law that refers to the Fundamental Charter is Law No. 19,733 on Freedom of Opinion and Information and Exercise of Journalism, (2001), which disregarded the mandate, since said legal text contains no rules regarding the treatment of personal data made by the mass media.

13 The bill was entitled: «Modifies article 13 of Law No. 19,628, on the protection of privacy, to establish the right to forget, personal data stored in search engines and websites», contained in the Bulletin No. 9388-03. It was presented to the Senate of the Republic on 11 June 2014 and was referred to the Committee on Economy, which in May 2017 had not yet prepared the respective report.

14 The parliamentary motion was called: Protection of personal data, commercial data, right to oblivion, protection of privacy, prohibition of the use of historical records, contained in Bulletin No. 9917-03, was presented on 10 march, 2015, as well In the Senate, and is currently on the Senate Economic Commission.

15 The initiative called, modifies Law No. 19,628, on the Protection of Private Life, in order to guarantee, to the holder of personal data, the right to forget, Bulletin No. 10608-07, was presented on 12 April 2016, is discussed in the Commission of Constitution of the Chamber of Deputies.

16 A synthesis of the most used search engines and their characteristics, see http://www.tnrelaciones.com/anexo/buscadores/

THE RIGHT TO BE FORGOTTEN IN CHILE

As of May 2017, a total of 30 protection actions against Google have been instigated, of which only two have been accepted. These are summarized below.

The first case was *Abbott Charme, Jorge vs. Google.cl and other*, and has some interest.[17] The action was not brought against Google, but against the entity that is registered in Chile, the domain name google.cl, so that the US Company did not appear in the trial. Also, because the Court of Valparaiso, in accepting the action, ruled that a measure was impracticable, both technically and legally, which we will explain later. The appellant was Jorge Abbott, the current Attorney General, who the year 2012, a protection against several websites. In such places, insulting and slanderous statements were spread about his person, spouse, children and family, which violated the constitutional guarantee of art. 19 No. 4 of the Constitution; respect and protection of the private life and honor of the person and his family. Among other things, he was charged with executing crimes against human rights and having committed acts of corruption in the exercise of the position of Regional Prosecutor of the Public Prosecutor's Office in the Valparaiso Region.

The Court of Appeal, in its reasoning, warned that the appellant and his family were affected by these sites, by the serious accusations against his honor and private and public life, by attributing to him the commission of offenses prosecutable ex officio or by accusing him of a lack of morality, which impliedly discredited the social appraisal of the appellant and his family, guaranteed and enshrined in art. 19 No. 4 of the Chilean Constitution. Therefore, the Court of Appeal of Valparaiso, welcomed the constitutional action, also issuing two measures that, in its opinion, would effectively protect the collapsed fundamental guarantee: -the elimination of the respective web pages described by the appellant of the injurious information - that the search engine "google.cl" establishes, computationally the necessary filters, to avoid publications that unequivocally present an offensive character, or of any type and under any circumstance, provided that such publication incurs a constitutional affectation as described. The second measure, not requested by the appellant, exceeded the Court's jurisdiction, by issuing an order of such general and broad character, unrelated to the lawsuit it was called upon to resolve. It also involves imposing on Google the adoption of a system of preventive control to the attacks against the right to honor, which would mean that the employees of that search engine were the judges on the content that could circulate on the Internet. Such a measure in short, it seemed to us, was unconstitutional and technically impracticable. This was demonstrated in the facts, as since the judgment of the Court of Valparaiso, Google has not adopted any filter and the court has not supervised the implementation of its decision.

The second case was *I.S.B. And others vs. V.F., Google Chile Ltda. and Google Inc.*[18] Three sisters and their aunt filed an appeal for protection against V.F., a man serving a prison sentence for the crime of child sexual abuse against the appellants. The respondent had created profiles on Internet sites between the years 2009 - 2013, to which the material that the affected considered malicious, defamatory and offensive was uploaded, requesting the elimination of such platforms. The Court of Appeals admitted that, not only were there expressions and photographs considered degrading by the aforementioned, but also recognized by the other defendant, Google Inc., owner of the digital media used to eliminate them, were degrading expressions related to sexual abuse and rape of which the respondents were victims and for which the author is condemned to 15 years of imprisonment and prohibited from approaching the victims for the same time as the sentence. Thus, the Court stated that maintaining the URL http://vril-novril.blogspot.com was aggravating for one of the appellants, contrary to their rights of psychic integrity and the protection of their honor, and, accepting the action, ordered Google Inc to delete the address and site http://vril-novril.blogspot.com. Both parties appealed the decision, although the Supreme Court did not decide the lawsuit, as both parties gave up when they agreed to a transaction that was not informed.

All other constitutional actions directed against Google have been rejected by the national Courts of Justice, on different types of both formal and substantive grounds. Regarding the former, they have been based on the filing outside the term of the appeal, which according to Chilean rules must be deducted within 30 days of the violation of the right. Because those affected usually ignore the time when content is uploaded and circulated on the Internet, the period in which the action is filed usually exceeds this deadline. Another line of case law dismisses the extemporaneity of actions based on the fact that as long as the contested content is maintained on the Internet, illegality continues to violate the rights of the affected, without the term can run.

Regarding the substance, the constitutional

17 Court of Appeals of Valparaiso, Case No. 228-2012, sentence handed down on 30 July 2012, which was not contested.

18 Court of Appeals, case number 1857-2015. Sentence dictated on 5August 2015. The ruling was appealed by both parties, cause Supreme Court role 11847-2015, although they resign.

THE RIGHT TO BE FORGOTTEN IN CHILE

jurisprudence has been homogeneous in founding the rejection of the actions of protection, on the arguments that Google contributes in its reports, that in strict is only one.[19] The Cortes maintain that the facts alleged by the appellants, -searches that the search engine sheds-, cannot be attributed to Google, because it is a company that provides services of searching pages on the Internet, and does not own the domain of some pages. This is the reason why it is impossible to eliminate information of the appellants that appears on the Internet. In line with this plea, Google suggests - and the courts have found so - that the appellants must direct their actions directly against the owners of the website that has published the information that it estimates affects their right to privacy and honor and physical and mental integrity, referred to in article 19 No. 4 and 19 No. 1. Some lawsuits have had a different reasoning. Thus, in *Kruljac, Daira vs. Google Chile and Google Inc.*, the Court deemed the offending of the contested publication was not indisputable. The court suggested that the appellant turn to Law No. 19,628 on Personal Data Protection, although it shared the other rejections, i.e. the recommendation to direct an action against the author of the content, as resolved by the Supreme Court in a ruling it cited. The cases *Gómez Arata, Maximiliano vs. Google Chile Ltda.* and *Google Inc. and Aguilera Aguilera, Verónica vs. Google Chile*, have a different reasoning, as the Cortes found rejection in a ruling handed down by the Supreme Court of Argentina, *Rodríguez María Belén c / Google Inc.,* which exempts search engines from monitoring content uploaded to the network, based on intellectual property law. In *Diaz with Google Inc.*, our courts invoked art. 85 P of the Chilean law on intellectual property, a rule like that of Argentina. A new argument was added in *Padrón Miranda, Margarita vs. Google Chile,* where the Court of Appeal, emphasizing the extraordinary precautionary nature of the appeal, indicated that it could not constitute an instance to clarify facts or establish responsibilities, for crimes that protect the honor of people. In other cases, as in *Carvallo Espinoza, Carolina vs. Google*, the courts have dismissed actions for having lost opportunity because the content that harms the affected no longer appears in Google searches.

V-LEGAL ACTIONS AGAINST WEB PORTALS OF PRINTED AND ELECTRONIC MEDIA

Twelve remedies have been filed against electronic media, of which two have been declared inadmissible because they have been interposed extemporaneously and, in the other, the appellant has given up.[20]

Nine lawsuits were sentenced considered in one case, and in one case, *Graziani vs. El Mercurio S.A.P.*, the Supreme Court upheld the action. The rejected actions were: *Olivares Barría, Daniel vs. Company El Mercurio de Valparaíso and others.*, Here, a surgeon doctor, also convicted of the crime of sexual abuse, required 5 years after his trial, the withdrawal of the news that reported on the criminal sentence 5 years after his trial. In *Warner Readi, María Isabel and another vs. Google Chile Limitada and others*, a former deputy required the withdrawal of news housed in the electronic version of the newspaper La Tercera published 4 years ago and that alluded to a conjugal conflict by the intervention of a former presidential candidate, which resulted in the marriage breaking up. The *Duran Portales Diego case vs. EMOL-El Mercurio SAP* and Google Chile, the appellant, who had been convicted of crimes against property, requireds the withdrawal of information published eleven years ago on his arrest and subsequent conviction. In *Covarrubias Llantén, Mario vs. COPESA S.A.*, a former policeman prosecuted for computer crime, who after the trial was favored with an acquittal, required the removal of the news published in the electronic version of the newspaper La Tercera eleven years later. In the case of *Medina Muñoz, Hernán vs. Grupo COPESA,* a surgeon requested the removal of a story published two years ago on the portal of the newspaper La Cuarta about alleged professional negligence, when operating on the wrong eye of an elderly woman. In *Millalonco Díaz, Juan vs. Google Inc.-Comercial The Clinic SA*, a lawyer required the removal of a news note, published in The Clinic 3 years ago, that reported on a civil action levied against an electronic journal that had reported on a fight Iin the public highway, for which he was convicted of inflicting injuries. In G*arfias Rabb, Claudio vs. Google*

19 *Aguirre Ornani, Elgor Loram vs. Google Chile cons. 5; González Canto, Ricardo vs. Google, cons. 5; Varas Bustamante, Gustavo vs. Google Chile cons.5 °; Venegas Cabrera, Ricardo vs. company Google Chile Limited cons. 5; Plaza Roco Gliciano with Google Chile cons. 6 °, and Wohl Escala, Ylan Ben vs. Google cons.* Four. In the case of *Gómez Arata, Maximiliano vs. Google Chile Ltda. and Google Inc.*, the reasoning is more synthetic, stating: 7) That in estimating this Court that Google Inc. is a search engine, that is limited to append publications which are uploaded to the website, without the supervision of such information (...). Very similar reasoning in *Gálvez Calderón, Carolina vs. Google Inc.*, (Motive 5°), in which also the Court of Appeals in founding the rejected, adds that the facts that the actress considered injurious were not based on antecedents of any species, at not even the place where such information appears indexed.

20. *Podesta, Julio vs. La Segunda on line, newspaper La Tercera, Emol.com, UPI.com and other media, C.A. Santiago,* Rol No. 28329-2013. 2. *Ibáñez Fuentes Omar, with newspaper La Cuarta and another*, rol n° 22975-2016. 3. *Méndez Alcayaga, Leopoldo con El Mercurio de Valparaíso*, rol N° 2828-2016.

THE RIGHT TO BE FORGOTTEN IN CHILE

Inc., Emol, Defensores.cl, and V / LexChile, the appellant, who had been convicted 12 years ago for the crime of drug trafficking, required the removal of the news in an electronic journal and of the judicial conviction. In *Vila vs. newspaper company La Tercera S.A. and others*, the appellant requested the disindexation of the journalistic notes to several electronic media that reported eight years ago on the appellant's theft and sexual abuse, for which he was convicted.[21] In the suit *Godoy Miranda, Roxana vs. The Red, UCV TV; TVN; Mega, CHV and Channel 13*, the widow of a homicide suspect - the victim was Hans Pozo - who then committed suicide, required all open television channels to eliminate news related to the crime. Lastly, in *Schwarze Luque, Antón vs. Televisión Nacional de Chile, La Red, UCV, Channel 13 and Mega*, a lawyer, who had been a government official, asked to suppressfor the suppression of news reports that had been reported two years ago about a fight with a neighbor, for which he was convicted of the crime of simple damages and threats.

The only action taken by the Supreme Court on the right to be forgotten was in *Graziani Le-Fort, Aldo vs. Empresa El Mercurio S.A.P.*,[22] a reason for which it has special importance.[23] For the first time in the judicial history of the country, the Supreme Court ruled on the merits of a lawsuit in which the applicability of the right to oblivion was discussed. This sentence decision seemed to us to be erroneous, as we shall explain, after synthesizing the case.[24] The appellant, deduced commenced an action of protection against the Company El Mercurio S.A.P. noting that, on October 6, 2015, it was verified that Internet search engines maintained a publication, which it had requested to eliminate the newspaper El Mercurio. The journalist's note, published in 2004 in the electronic newspaper emol.cl -belonging to the journalistic company- reported that a judge had submitted to trial, as an alleged perpetrator of sexual abuse against minors. Graziani was at that time a major retired Carabinero, adding that such events occurred more than 10 years ago and that while at that time he complied with reporting, today he is damaging day by day his right to psychological integrity is being damaged day by day. The complainant maintained that, on August 21, 2015, he presented to the company El Mercurio a letter requesting it to remove from the search engines the aforementioned notice. The newspaper demanded valid documents proving the dismissal, acquittal, or other and the signing of a termination of resignation of any legal action against the media or director, a response, which, for the appellant, generated a conflict. He maintained that the actor's right to psychological integrity was also violated, due to the development of current life together with technology, so that if third parties want to hear from you, the publication will appear, aggrevating the situation for those now suffering health problems, which could even cause death. He therefore asked for the removal of the news from the Internet search engines in which it appears. El Mercurio, in its report, admitted to having published the news, which fell on a public fact, spread by the country's media. The media added, which that the written media, are used by Internet portals to inform the respective news search engines, so it is not possible to delete such information, because doing so without justifiable cause, would be contrary to the freedom of information basis of the exercise of journalism. He pointed out the defense of El Mercurio, that the legitimate exercise of freedom of information, making real facts known, was also guaranteed by the Chilean Constitution, in No. 12 of art. 19, so that the rights of the appellant could be unlawfully or arbitrarily affected. The newspaper appealed that, because there are other ways to complain, -a clarification or rectification procedure in the press law, and the removal of criminal records by the Civil Registry-, the action of protection was impertinent. The media admitted that to eliminate a news story are needed to justify the measure needed to be justified, stating that the only search engine that depends on El Mercurio is emol, but no other can order or instruct the removal of certain information, calling for the rejection of the appeal.

The Court of Appeal, in its reasoning, stated that the news object of the resource published on the site emol.com was made by the media about facts that were judicially accredited by investigating judge, Sergio Muñoz, who substantiated said case and that, in the present action, were recognized as effective expressly by the appellant.[25] In the operative part of the decision, the court considered that it was not possible to describe as "arbitrary or illegal the publication of the journalistic news of which the appellant was subject, even though more than 10 years have elapsed since this occurred in the exercise of freedom of information without

21 The affected one filed an appeal to the Supreme Court, rol N° 11746-2017, which is currently in the process.
22 Court of Appeals of Santiago, Case No. 88640-2015. Revoked by the Supreme Court, Case No. 22,243-2015.
23 A brief analysis, critical of the methodology and use of sources in the ruling issued by the Supreme Court, see, The Fundamental Right to forgotten in the Web and the Chilean Constitutional System, in Constitutional Studies, year 14, No. 1, 2016, p. 309-318.
24 Acciones Constitucionales contra Google, ANGUITA RAMÍREZ, Pedro, editorial Librotecnia, Santiago, Chile, p. 101-103
25 Considering Sixth. Eliminated by the Supreme Court.

THE RIGHT TO BE FORGOTTEN IN CHILE

prior censorship, being a fact of public knowledge by various means of communication".[26] So, for the Court of Appeal, "the information currently maintained by the site EMOL.COM, corresponds to a real and certain news, confirmed by the actor himself in his libel, regarding an unlawful act that he committed and was investigated for in the context of the Spiniak case and for which he was put under trial." In this regard, the Court added that the appellant did not prove by any means of legal proof, the current procedural situation or, a change of circumstances and could modify the current circumstances. For this reason, the Court found that the defendant did not violate the guarantee of the right to psychological integrity, equality before the law and protection of privacy and honor of the appellant, when reporting truthful facts in the exercise of their role and constitutional right. Neither, warned the Court, was there a collision of fundamental rights, because the news published by the respondent, in the exercise of freedom of information, was recognized as true by the appellant himself.[27] Finally, the Court of Appeals saudthat the appellant could exercise the actions contemplated in Law No. 19.733, if he considered that the publication violated his fundamental rights. From such reasoning, the Court of Appeals unanimously decided,to reject the appeal against the newspaper El Mercurio.[28]

The Supreme Court, in a divided decision, revoked the decision of the Court of Appeals, eliminating the operative part of its decision.[29] In the operative part, Laema argued that the right to be forgotten was not new, since, in particular, foreign jurisprudence elaborated criteria that according to which the legislation established to resolve these conflicts, as in the case of criminal law, where the right to forget was developed for the first time. In this sense, our highest court of justice explained that in the event of a conflict between the right to forget about the judicial past -penal precedents and past convictions- and the right to information -access to said information-, the time factor is a decisive criterion, enabling the right to information to prevail in case the information has a journalistic interest, due to its relevance. Otherwise, the right to forget will prevail over the right to information, being able to allude to the sentence, but without the names of those involved. The highest court in the country estimated that maintaining a news story as the case motivated, after a decade, was extraneous to the purpose of informing the public of the events that occurred at that particular time, which showed greater interest and utility. The Supreme Court reasoned that if the penal law, which is the most serious in affecting individual rights, has a specific length of time for punishment, and also allows it to be eliminated from all public records once it has been complied with, even more so the social media should act coherently with the intention of giving the prisoner the possibility of developing a life in accordance with the respect of their constitutional guarantees, after the time of conviction. The Supreme Court highlighted the passage of more than ten years since El Mercurio announced the news about the participation the appellant had in a crime of particular social relevance, which later featured in the search engines of the digital versions of the newspaper, and attributed it "to the scrupulous record of its history of news", constituting for the court, a legitimate exercise of its right to expression, also protected by the same Constitution. The High court dismissed that there was a collision between constitutional rights, and that if it existed, it had to cede in favor of the right to social reintegration of the person who had committed it and of its right to maintain a private life that allows it, as well as the right to honor and privacy of his family, in the surname suit to be easily approachable and unique. We do not allow our maximum court of justice, the current benefit of freedom of expression, to maintain a digital record detectable by any computer search engine of,a news that can be consulted by analogous methods, through the professional investigative exercise of those who are interested. The Supreme Court held that the aim is not to provide automatic access to facilitators that make it more difficult or impossible to recover and reintegrate the individual and his family, but, if the latter should never be affected, the aim is not that the news should stop to exist. In the final part of its reasoning, the country's highest court of justice estimated that more than ten years from the date of the news - sufficient time for the criminal prescription of most of the most serious crimes - was more than enough to resolve provisionally and cautiously the aforementioned constitutional guarantees, that the computer "oblivion" of the records of said news must be procured. The Supreme Court overturned the ruling issued by the Court of Appeals, accepteding the action and ordered the newspaper El Mercurio to delete the computer record of the news that adversely affects the appellant, within a period of three days. The ruling had an extensive and founded minority vote that was for rejecting the action.

26 Considering Seventh. Eliminated by the Supreme Court.
27 Considering Eighth. Eliminated by the Supreme Court.
28 Considering Eighth. Eliminated by the Supreme Court.
29 The judgment re-produced to itself in appeal, with exception of his foundations sixth to ninth, that are eliminated.

THE RIGHT TO BE FORGOTTEN IN CHILE

VI-EPILOGUE

The lawsuits filed in Chile, which have aimed to eliminate content circulating on the Internet based on the right to be forgotten, are often dismissed by the national courts of justice, with some qualified exceptions. This jurisprudential practice has included both legal actions directed against Google, as well as digital media, newspapers, magazines or television channels that have digital platforms where they host their content.

The Supreme Court of Chile has recognized only in the Graziani case the so-called right to be fortgotten. In that trial, the country's highest court established a debatable standard in recognizing such a right for a person sentenced for crimes of sexual abuse of minors, ordering the deletion in their digital archive, of a journalistic note published eleven years ago that the appellant had been tried for these crimes. The time elapsed between spreading and serving time was three years. According to this criterion, any person who in the country that has been convicted, or only imputed, formalized and especially acquitted of any crime, may require the suppression of all news related to illegal acts stored in the digital archives of a medium of communication. The deadline calculated in the case Graziani, determined by the Supreme Court, was to account for the period from the time the article was published that reported on the ruling of the judicial process, that submitted to the appellant until the date of filing the action for protection, which required the elimination of such information, was eleven years. As for the substantive reasoning of our country's highest court of law in the Graziani case, we will say in summary that it did not determine what the illegal or arbitrary act was and did not state what the appellant's violated right was, which, under unanimously supported jurisprudence, constitute the essential prerequisites for the application of protection, in accordance with the clear tenor of the enumeration made by art. 20 of the Chilean Constitution.

The doctrine elaborated by the Supreme Court in the Graziani case, a judgment handed down in January 2016, which recognized the right to be forgotten in a debatable case, has not been exposed again, neither by the Courts of Appeal, nor the Court itself Suprema has ratified the decision in that lawsuit.

Finally, it would be very interesting for cases on the right to forgotten such as Graziani against El Mercurio to be known by the Inter-American System of Human Rights, to evaluate the compatibility of this right with art. 13 of the American Convention on Human Rights.

THE RIGHT TO BE FORGOTTEN FROM THE MEXICAN EXPERIENCE

By Olivia Andrea Mendoza Enríquez
Full-time Research Professor at the Public Research and Innovation Center in Information and Communication Technologies INFOTEC.

Talking about new rights configured from the digital economy is increasingly common, attending to technological development. One such example is the so-called right to be forgotten. The concept of the right to be forgotten, originates from the already well-known right to personal data protection - recognized in several Ibero-American laws - and finds its relevance for analysis in the recent position of some courts and the need to incorporate it into the national legislation. However, some particularities should be emphasized with the right to be forgotten, especially in the digital age, since its guarantee could propitiate some violations of other rights, such as expression freedom, the right to truth and access to information.

In light of the above, it is pertinent to analyse in the following lines the origin of the right to be forgotten, the reflections that have taken place in Mexico regarding the subject, the position of the institution in charge of guaranteeing the data protection and the legislation about this right, with the aim of giving the reader an overview of this right in the Mexican legal system.

I-PREVIOUS CONSIDERATIONS

When we speak of the right to be forgotten, we must remember that this right has its origin in Judgment T-414 of June 16, 1992, issued by the Constitutional Court of the Republic of Colombia, as well as its incorporation into national legislation, such as the case of Article 10 of Law 787 of 2012 of the Republic of Nicaragua and Article 11 of Decree 37554 of 2012 of the Republic of Costa Rica.

On the other hand, although the right to be forgotten is not recognized, the right to de-indexation has its origin in two main sources: the *Google Spain* case of 2014, settled by the Court of Justice of the European Union (in which the search engine was required to eliminate certain results of information) and recently in the General Data Protection Regulation of the European Union.

Since then, more Latin American countries have raised the need to include the right to oblivion in their national legal systems, which is explained, among other things, by the need to achieve optimal levels of information protection, requirements to perform transfer of data, or establish commercial acts.

The right to be forgotten is directly related to the conception of the personal data protection right that we have from the countries that integrate the Roman-Germanic legal family, so the dimension of this right, will be different with respect to the countries that integrate the legal family of the common law, since for them the data protection is not a human right or fundamental right, it is a consumer right, regulated sectorially. This factor must be considered because the majority of searchers have their origin in countries of this last legal tradition.

On the other hand, the first antecedent of the right to be forgotten in Mexico, is in the position of the National Institute of Transparency, Access to Information and Protection of Personal Data (INAI), regarding a request for protection of rights formulated by a Mexican citizen, which we will analyse in the next section.

THE RIGHT TO BE FORGOTTEN IN MEXICO

II-FIRST APPROACH TO THE RIGHT TO BE FORGOTTEN IN MEXICO

The INAI guarantees the right of data protection in Mexico and announced in 2015, a punishment against Google Mexico, since this search engine did not fulfil a request for the exercise of the right of cancellation of data from a Mexican citizen. The same institution ordered Google to remove information links relating to this person, referring in its argument to the so-called right to be forgotten[1].

This request was instigated by a Mexican entrepreneur, who first asked Google to remove several search results related to his name, saying that the information affected him in the most intimate sphere and also his current financial relationships, since one of those links was about the newspaper report 'Fraud in white star company, affects to Go México institution', published in 2007 by Fortuna magazine. In this note, the entrepreneur is mentioned as one of those implicated in acts of corruption.

Mexican legislation on data protection in the private sector, says that in the case that the request for cancellation rights is not fulfilled by the private actor (in this case Google), the data owner may request, through the so-called request of data protection, the guarantee of his right, in order to start an investigation and just in case, start a procedure against the private actor.

One of the arguments that the search provider (Google) gave to the authority, in relation to the non-cancellation of the data, was not having the faculty to determine the type of information that could be indexed in the search engine, since Google was not responsible for the information in the original source.

This was a unique opportunity to influence the construction of the right to be forgotten in the country since, on the one hand, the searcher was assigned an administrator role in relation to the accessibility of information through the Internet -determining the relevance of the information and having the power to affect Internet neutrality and, on the other hand, civil society was concerned about the effect on the right of freedom of expression.

In this regard, the Mexico office of Article 19, stated that the act of deleting the links to the note (despite not deleting the information in its original source), established a censorship.

When presented with the unique opportunity to establish the first precedent of the right to be forgotten in Mexico, an organization called the Digital Rights Defense, requested Fortuna magazine (the electronic media that was the original source of information) to promote a legal action against the decision of the data protection institution, since despite all the analyses described, the institution never informed the magazine about the effect that the decision (de-indexation of the journalistic note from the Google search engine) was going to have, regarding the measure of censorship imposed.

In the first instance, an administrative court dismissed the process.The organization of civil society was discontent after the refusals and the case was moved to another court, which a year and a half later left without effecting the historic resolution of the National Institute that protects the personal data.

The legal strategy consisted in promoting an amparo petition for violation of the rights of freedom of expression and guarantee of hearing. Google, for its part, challenged the resolution issued by the authority, which guarantees the protection of personal data in Mexico (INAI), and filed an appeal in the Fiscal and Administrative Court of Justice.

The Federal Constitutional Court rejected the constitutional complaint and Fortuna Magazine requested a review of the decision, and at second instance (Collegiate Court), the appeal was granted because of due process considerations (right of hearing). With this, the original resolution of the INAI was left without any effect and INAI was ordered to start a new procedure, guaranteeing rights for those involved.

III-A NEW DISCUSSION

In 2016, the public discussion about the right to be forgotten emerged again, to analyse, in the Senate of the Republic, the need to incorporate this right expressly in legislation on personal data protection. Faced with this discussion, a call was made to experts from academia, industry, and the public sector, in order to discuss the dimensions of this right[2]. One of

1 http://inicio.ifai.org.mx/pdf/resoluciones/2014/PPD%2094.pdf

2 http://comunicacion.senado.gob.mx/index.php/informacion/boletines/30363-analizan-senado-e-inai-alcances-e-implicaciones-del-derecho-al-olvido.html

THE RIGHT TO BE FORGOTTEN IN MEXICO

the principal approaches identified was the need to inform individuals that the guarantee of the right to be forgotten could be derived from the other human rights such as freedom of expression, the right to truth and access to information, and that tension of rights is resolved through the necessary deliberation of the guarantee of the right to be forgotten.

In this sense, one of the most common examples is related to the enforceability of the right to be forgotten, versus the rights to freedom of expression, or access to information on the Internet. Here a variety of factors will be considered such as, the degree of public exposure of the applicant, if it is a question of incorrect information, if it involves a child or adolescent, or if the request violates the dissemination of information of public interest.

In addition to the above, it is emphasized that in Mexico reference has been made to the concept of the right to be forgotten refering to the elimination of information in cyberspace, but, in the author's opinion, we are instead facing a "right of non-indexation." Since, so far, search providers have been required to de-index information, but the original sources have not been forced to suppress information. An exception to this, refers to a request for the right to be forgotten in Colombia, in which a citizen asked Google to eliminate search results that related to an investigation of human trafficking, in which she was later found not guilty. The Colombian justice, instead of ordering Google to de-index the information, ordered directly that the information medium clarified in another note that the investigation determined the the holder of the request's lack of responsibility for the crime mentioned. That is to say, it does not violate the right to the truth - a person was involved in a human trafficking investigation - but in an explanatory note, it should be stated that she was not found guilty by the competent authority[3].

IV-RIGHT TO BE FORGOTTEN FROM THE MEXICAN EXPERIENCE

Data protection in Mexico has a hybrid model that dictates provisions through two particular laws; the first applicable to the public sector and the second to the private sector. In addition, there are some normative provisions at sectoral level, for example provisions for financial, health, and fiscal data.

Currently, the federal law that protects personal data in the private sector recognizes the so-called ARCO rights (right of access, rectification, cancellation and opposition of personal data). For the purposes of this analysis, the last two rights pursue the same objectives as the right to be forgotten in spite of not being mentioned under this name; data legislation for the private sector recognizes the right to cancel information or oppose the treatment of it.

On the other hand, according to the recent Law of Data Protection for the public sector, the right to cancel personal data must be guaranteed, provided that; the causes that motivate requesting the deletion, are indicated in personal data in registers or databases of the person responsible for the information and the right of opposition to the processing of personal data, provided that the holder of the information shows legitimate causes or the specific situation that motivates the request for cessation of treatment, and the damage or prejudice caused by the persistence of the treatment, or, if applicable, the specific purposes in respect of which it requires the exercise of the right of opposition.

In the legislation of the public sector, the following limits are established for the exercise of the right of cancellation or opposition:

- Not certifying ownership of the data, or due legal representation to request the cancellation or opposition of the information.
- When there is a legal impediment (Example: In the case of the refusal of requests for cancellation of data related to the obligation of an authority to treat information derived from one of its faculties conferred by law).
- When judicial or administrative proceedings are affected.
- When there is a resolution by a competent authority that restricts access to personal data or does not allow the cancellation or opposition of the same.
- When necessary to protect legally protected interests.
- When necessary to comply with legal obligations (Example: request the cancellation of data related to a credit granted by the Mexican State).
- When, based on their legal attributions, daily use, shelter and management are necessary and proportional to maintain the integrity, stability and permanence of the Mexican State.
- When personal data form part of the information of the financial entities regulation and supervision.

3 https://www.ambitojuridico.com/BancoConocimiento/Educacion-y-Cultura/noti-141809-04-derecho-al-olvido-y-lista-clinton

In the event of a refusal by any representative of the Mexican State regarding the cancellation or opposition of personal data, the owner of such data may go to the guarantor authority through an review appeal, so that specialized institution can determine if the refusal is in accordance with that provided by the standard, or if applicable, order the guarantee of these rights.

Another important aspect is that according to the data law of the public sector, the data in possession of the Mexican state must comply with the standard of quality. It is understood that this principle depletes when they have been provided directly by the data owner and until otherwise stated.

V-CONCLUSIONS

As a conclusion of this analysis, we say that the right to be forgotten cannot be guaranteed in a general way, since categories must be established, such as those related to personality rights, property rights, or information freedoms. In addition, in traditional law, there are legal rights that could help against the disclosure of excessive, erroneous or incorrect information. Examples of this are the right of reply, the right to own images and civil compensation for moral damages.

It emphasizes the need to refrain from dictating general rules in guaranteeing the right to be forgotten and to deliberate human rights that are in dispute.

In addition, the law should differentiate the figure of the intermediary with that of the person responsible for the data disclosed by users. In the same sense, legislation should guarantee control over the procedure against excessive information elimination, in order to have a balance between the traditional protection granted to rights such as freedom of expression and the right to the truth in relation to the arguments related to the privacy and protection of personal data.

In the same sense, under the premise of global thinking and local action, Internet neutrality should be favored.

Finally, note that the information that is made available through cyberspace can be replicated in many other sites, so having control of it is not easy.

CURRENT SITUATION OF DISCUSSIONS ON THE RIGHT TO BE FORGOTTEN IN JAPAN

By Shizuo Fujiwara
Professor, Chuo Law School, Chuo University
Areas of Specialization: Administrative Law, Information Law, Local Autonomy Law

Since the *Google Spain* decision, requests for deletion of search results were successively sent to district courts even in Japan. It exceeds 50 cases. On January 31 2017, the Supreme Court of Japan showed the judgment standard for the first time. According to the decision of the Supreme Court, compared to the social significance of the display of the search results, 'deletion is permitted if privacy protection of the individual is clearly superior.' The Supreme Court stated that the content of the information, the extent of the damage, the social position, and other factors should be taken into consideration in the judgment. As a result, in the case of child prostitution, the Supreme Court dismissed the men's appeal by referring to freedom of expression. The Supreme Court did not mention 'the right to be forgotten'. In Japan, similar discussions have been taking place since the 1980s. Traditionally, in Japan, the view, that understands that the right to be forgotten is not regarded as an independent right and is not more than the right to erase, is dominant. Unlike the EU, in Japan, few people argue the legislation theory on forgotten rights, rather Japanese administrative agencies recommend vendors' voluntary efforts. In fact, there are also search service providers who publish voluntary deletion criteria.

Computers Don't Forget. However, people are able to forget things. Leaving aside the details of neuroscience, people forgive each other and are forgiven through the process of forgetting. They are able to make a break with the past. Computers, however, do not forget. In the Information Age, computer networks are woven around us like the threads of a spider's web, and the personal information that gets caught in them is not forgotten. As a result, worries that the follies or pranks of youth could come back to haunt us when we go job-hunting or enter the workforce are becoming a reality.

In introducing the so-called personal data protection general rule, a proposal of the EU made public in January 2012, I explained 'the right to be forgotten' using the above sentences.[1] However, in Japan, the *Google Spain* judgment triggered the recognition of 'the right to be forgotten' among the people. The *Google Spain* judgment was widely reported in Japan, and thereafter, in Japan, requests for removal of search results were successively sent to the district court. According to the Supreme Court, the number of complaints to the district court nationwide regarding the deletion of search results was 52 in one year up to September 2016.

I-THE ISSUES IN JAPAN

If 'the right to be forgotten' included the right to seek protection from the report of criminal facts, such rights have long been discussed in Japan as well. Even if the entity of this right is the right to delete, in Japan, the grounds have already been established in the ordinance of local public entities 30 years ago. After the *Google Spain* decision, discussions have been made after grasping 'the right to be forgotten' as a right to delete search results from search companies.

Currently, the problem in Japan[2] is infringement of

1 Shizuo Fujiwara , The Right to be Forgotten and Policies for the Protection of Personal Information, ChuOnline 2012, http://www.yomiuri.co.jp/adv/chuo/dy/opinion/20121119.html

2 In Japan, news by newspaper companies and television stations are automatically deleted in a short period of time after they are

the rights of arrested persons, suspects and victims of crime through writing to anonymous bulletin board based overseas, reprint to the same type of bulletin board, and long-term posting. Since these are displayed as search results, a request to delete search results is made.

II-SUPREME COURT DECISION OF JANUARY 31, 2017

A-FACTS

X was arrested in November 2011 based on charges of child prostitution and was sentenced to a fine in December of the same year. The fact that X was arrested was reported on the day, after which it was reprinted in many electronic bulletin boards etc. Even when three years or more have passed since the child prostitution act and even if more than three years have elapsed from the summary order, when people search Google with the name of X and the prefecture name where they reside, they can see a link to those sites and an excerpt of relevant parts of the site. Therefore, in January 2015, X requested Google to delete these search results based on personal rights (right not to hinder rehabilitation).

The first instance, Saitama District Court decision (June 15, 2015, December 22, 2015) admitted the order of provisional disposition by referring to 'the right to be forgotten' for the first time in Japan. That is, 'people have the right to forget people from past crimes after a certain period of time.' On the other hand, the Tokyo High Court, on July 12 2016, revoked the original decision and dismissed the petition for temporary disposition of X.

B-KEY FEATURES OF THE SUPREME COURT DECISION ON JANUARY 31, 2017

The main points of this decision are the following:

- The profits that are not publicly disclosed to the facts belonging to the individual's privacy should be subject to legal protection.
- The searcher collects the information posted on the website on the Internet comprehensively, preserves its copy, and organizes the information by creating an index based on the copy. Then, the search provider provides information corresponding to a certain condition indicated by the user as a search result based on the index. Although the collection, arrangement and provision of information is carried out automatically by the program, since it was created so that the result can be obtained according to the policy of the search provider concerning the provision of search results, the provision of search results has an aspect of expressive acts by search business operators. In addition, providing a search result by a search provider supports the public to transmit information on the Internet and obtain necessary information from a huge amount of information on the Internet . In other words, in modern society it plays a big role as the basis of information distribution on the Internet. And if the act of providing a specific search result by a search provider is illegal and it is forced to delete the search result, such a situation brings two constraints to the operator. It will not only constrain consistent expressive behavior of the business operator but also restrict the role that the business operator plays through providing the search results.
- Given the nature of the search activity provided by the search provider as described above, whether or not the acts offered as search results are illegal should be judged based on the following criteria. It should be judged by comparing the legal profit that does not disclose the facts and the circumstances that provide the URL etc. information as search results. The main criteria here are: (1) the nature and content of the facts, (2) the extent to which facts belonging to that person's privacy are conveyed as a result of the provision of the URL etc. information, the extent of the specific damage incurred by the person, (3) the social status and influence of that person,(4) the purpose and significance of the above-mentioned article etc, (5) the social situation and the subsequent change when the above-mentioned article etc. was published, (6) the necessity to describe the fact in the above-mentioned article etc.
- If it is clear that the legal benefit not disclosed is superior as a result of comparative equilibrium, it is understood that the search provider can be requested to delete the URL and information from the search result. In this case, the appellant had requested that the search results be deleted on the grounds that articles containing all or part of the facts are posted. Indeed the fact that he was arrested on the grounds of suspected child

posted on the Internet, so it is unlikely that deletion requests will become a problem. In addition, in Japan relief for privacy infringement has been developed under the Act on Tort Law of the Civil Code.

THE RIGHT TO BE FORGOTTEN IN JAPAN

prostitution is a fact belonging to the appellant's privacy, he not wanting others to know. However, in light of the fact that child prostitution is regarded as sexual exploitation and sexual abuse against children, it is regarded as a subject of strong social condemnation and is prohibited with penalties, it is still a matter concerning the public interest at the present time. In addition, since the search result is part of the search result in the case of the name of the prefecture in which the appellant resides and the name of the appellant, the range in which the fact is conveyed is limited to a certain extent. Based on the above comparative consideration, taking into consideration circumstances such as the fact that the appellant lives with his wife and child and has operated a private company without committing a crime for a certain period after being imprisoned for a fine penalty, it can not be said that the legal benefits that are not publicized are superior.

C-COMMENTS

- The Tokyo High Court ruled that the substance of 'the right to be forgotten' is not different from «the right to demand an injunction based on the honorary right or privacy right as a content of moral rights.» It clearly denied 'the right to be forgotten' in its own right. This point is also the way many Japanese lawyers think. The Tokyo High Court also refers to the following points. That is, if the search result is deleted, not only the description concerning the crime but also the entire web page of the link destination becomes difficult to read, which means that the freedom of expression and the right to know can be greatly infringed.
- The Tokyo High Court judged mainly the infringement of honor rights, but the Supreme Court judged it as a matter of infringement of privacy.
- The Supreme Court of Japan did not mention 'rights to be forgotten'.
- The Supreme Court unveiled for the first time the legal position of acts of search businesses. According to it, 'providing search results has aspects of expressive acts by search companies themselves.' Therefore, providing search results involves responsibility as expression acts, but at the same time it is guaranteed as freedom of expression.
- The Supreme Court acknowledged that the provision of search results 'played a major role as a foundation of information distribution on the Internet in modern society.' This is an argument discussed as a matter of the right to know in high court decisions etc.
- As far as deletion is concerned, the Supreme Court stated that it is only acceptable if privacy does not merely dominate privacy but it is obvious. It can be evaluated that the deletion obligation was accepted only limitedly. This is probably because the act of providing search results is an expressive act, related to freedom of expression, and the importance of the social role of business operators in information society was recognized.
- There is criticism against the Supreme Court ruling that it is disregarding the damage of privacy infringement. However, regarding the problem of deleting the search results, it is a matter of whether or not a search provider who is not a sender should conduct relief of privacy infringement. Considering the viewpoint of freedom of expression and right to know, the Supreme Court has concluded that it should be cautious about this.

III-SELF-REGULATION

Unlike the EU, there are not many people in Japan discussing the legislative theory about the rights to be forgotten. As already mentioned, there are many who think that it is possible to sufficiently deal with the deletion right stipulated in laws and ordinances. Some people are skeptical as to whether the term 'the right to be forgotten' has more content than the symbolic meaning. Rather, the administrative agency in Japan recommends businesses' voluntary efforts. It is a method called administrative guidance which is often used when Japanese administration thinks to induce business operators. Administrators dislike the cost of making laws, and operators prefer soft regulations of self-regulation over hard regulations of law. In fact, there are also search service providers who publish voluntary deletion criteria.

IV-CONCLUSION

The Japanese Supreme Court silenced 'the right to be forgotten.' On the theory, 'the right to be forgotten' is still a controversial right, not an approved right. However, since the Supreme Court ruling on January 31, 2017, the number of papers discussing the right is increasing, and the discussion will be refined in the future.

THE RIGHT TO BE FORGOTTEN AND ITS RAMIFICATIONS IN TAIWAN, CHINA AND JAPAN

By Hsu, Piao-Hao
Lecturer at International School of Technology and Management, Feng Chia University, Taichung

The *Google Spain* Judgment from the Court of Justice of the European Union on the right to be forgotten (RTBF) in 2014 has generated an enormous echo all over the globe. To examine the normative influence of the EU as well as how the RTBF has unfolded in regions where values of privacy differ, the RTBF cases in Taiwan, China and Japan are presented and compared. Though still preliminary, this short article found that to successfully claim RTBF in jurisdictions where the concept is still novel, if not strange, emphasis on the harm to privacy is essential.

Today, connected devices and the internet have filled up almost every moment of our life. All of us leave countless footprints in the world of the internet each second. Nevertheless, compared to human beings, who have the inherent functioning of forgetting what has been put into our minds, the internet never forgets. Yet we, people who live in the real world, do not always welcome people's learning of our past through the sometimes timeless internet, that we ourselves might want to forget.

On May 13, 2014, the Court of Justice of the European Union (hereafter: the CJEU) announced its judgment on Case C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD)* (hereafter: the *Google Spain* Judgment).[1] The Judgment further elaborated on the scope of Data Protection Directive (Directive 95/46/EC),[2] and was deemed to have set up "the right to be forgotten" by the media.[3] According to the judgment, when the processing of a certain piece of data related to a data subject becomes "inadequate, irrelevant or no longer relevant, or excessive" over the course of time, the operator of the search engine then bears the obligation, upon the request of the data subject, to consider the interests involved in each case, such as the interest of the general public in having access to that information upon a search relating to the data subject's name, and to decide if it should erase information and links concerned in the list of results in the case.

Within 5 months after the *Google Spain* Judgment, Google received more than 18,000 requests in the United Kingdom alone and 145,000 in the whole of Europe, to delete related information from the search results (29,000 requests in Germany and 25,000 in France).[4] Currently, for anyone who wishes to exercise his or her "right to be forgotten" as reckoned by the CJEU, he or she has to go through several layers of "guidance" and come to the page where one can eventually fill out the application.[5]

In addition, other search engines such as Bing have also started to provide a similar service on their web pages for European residents to apply for their names to be removed from the search results.[6] Moreover, discussion

1 Case C-131/12 *Google Spain SL, Google Inc.v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*" [2014] ECLI:EU:C:2014:317

2 European Parliament and of the Council Directive 95/46/EC 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] O. J.L 281/31

3 Alan Travis & C. Arthur, 'EU court backs "right to be forgotten": Google must amend results on request.' *The Guardian* (London, 13 May 2014) < https://www.theguardian.com/technology/2014/may/13/right-to-be-forgotten-eu-court-google-search-results > accessed 25 May 2017

4 'Britons ask Google to delete 60,000 links under "right to be forgotten"' *The Guardian* (London, 12 October 2014) <http://www.theguardian.com/technology/2014/oct/12/google-60000-links-right-to-be-forgotten-britons> accessed 25 May 2017

5 'Remove information from Google' (Google) <https://support.google.com/websearch/troubleshooter/3111061> accessed 2 May 2017

6 'Request to Block Bing Search Results In Europe' (Bing) <https://www.bing.com/webmaster/tools/eu-privacy-request> accessed 25 May 2017

THE RIGHT TO BE FORGOTTEN IN TAIWAN, CHINA AND JAPAN

over the right to be forgotten has emerged in all over the world, including the U.S.,[7] Canada,[8] Japan,[9] Hong Kong,[10] Taiwan and other non-EU zones. Local cases, for example, have also taken place in Taiwan and other non-EU jurisdictions, where individuals requested the search engine operator to delete certain links in the search results after typing in his name.[11]

Between 2015 till present, a number of cases related RTBF emerged in Asian countries such as Taiwan, China and Japan. It is interesting to see how the normative power of the EU manifests itself in the form of other than legislation, but also in the form of "live" jurisprudence thanks to the facilitation of the internet and globalization. In this short article, three cases are chosen respectively to represent the current development of RTBF in the abovementioned Asian jurisdictions. To conduct a more wholesome analysis, the legislative frameworks of these countries shall also be considered. Nevertheless, due to the limit of length, the present article focuses on presenting an overall picture of the influence of the 2014 *Google Spain* Judgment in jurisdictions outside the EU-zone by highlighting the most recent cases.

I-RTBF CASE IN TAIWAN

After the *Google Spain* Judgment, a comparable case also took place in the Taiwanese Courts. In October 2008, the Liberty Times (a major local media outlet) reported news with titles such as "Shi Jiang-Xin Not Board Member of MiDiYa" and "Financially-related to Mafia, Head of MiDiYa Involve in Baseball Fraud". The news coverage mainly reported on the prosecutor's investigation of Mr. Shi Yu-Zhe (original name: Shi Jian-Xin)'s alleged involvement in the illegal bets and related fraud on professional baseball games in Taiwan.[12] Yet, as regarding to Mr. Shi' being accused of committing fraud in this specific case, he has been declared not guilty by the High Court of Taiwan in January, 2013.[13]

Later, in the Civil Affair Judgment Case Su Zi No. 2976 of Taiwan Taipei District Court, Mr. Shi, the plaintiff of this case, made several claims that could be classified as the exercising of the right to be forgotten. In his claims, Mr. Shi indicated that if an internet user uses "Shi Jiang-Xin" as a keyword to search within the search engine product "Google Search" of Google International LLC registered in Taiwan, a number of pages where the content of the abovementioned Liberty Times news coverage was reposted as well as more pages containing malicious defamation content based on the news coverage would show up in the search results.

Mr Shi thus requested the defendant, the Google International LLC, to first remove all the search results as listed in the appendix of his claim, which showed up after typing in the name of "Shi Jiang-Xin" as the keyword in the Google Search, and to secondly remove the suggested keywords "Shi Jiang-Xin Fraud Baseball" on the web page of "http ://www .google .com .tw". For those claims, the plaintiff has cited the judgments from the CJEU, Tokyo Court in Japan, and Article 184, 213, 195 of Civil Code of Taiwan and Article 7, 8 ,9 of Consumer Protection Law as the bases of his claims.

In an earlier court proceeding of this case, the Taipei District Court decided in its judgment announced on January 16, 2015, that the defendant is not the subject who committed tortious acts. In supporting its reasoning, the District Court noted, that "it is possible to use Google Search in Taiwan, but it cannot be concluded, accordingly, that the data was collected and organized within our country (Taiwan). Therefore, the defendant (Google International LLC), who is registered in our country, cannot be deemed as competent at and responsible for managing the Google Search engine, just due to the mere fact that Google Search engine is available for being used in Taiwan."

7 'Debate: Should The U.S. Adopt The 'Right To Be Forgotten' Online?' *National Public Radio* (Washington, 18 March 2015) <http://www.npr.org/2015/03/18/393643901/debate-should-the-u-s-adopt-the-right-to-be-forgotten-online> accessed 25 May 2017

8 Andre Mayer, 'Right to be forgotten': How Canada could adopt similar law for online privacy' *CBC News* (Ottawa, 16 June 2014) <http://www.cbc.ca/news/technology/right-to-be-forgotten-how-canada-could-adopt-similar-law-for-online-privacy-1.2676880> accessed 25 May 2017

9 Wasurarerukenri mitomerarerudekeka Google Kensatsukek-ka Yihoukette notoutouseiha' *The San Kei Shimbun* (Tokyo, 29 October 2014) <http://www.sankei.com/economy/news/141029/ecn1410290004-n1.html> accessed 25 May 2017

10 'Yin Si ZhuanYuan Yu Tui Bei Yi Wang Quan You Da Yan Lun Ji Xin Wen Zi You' *Inmediahk* (Hong Kong, 16 April 2015) <http://www.inmediahk.net/node/1033436> accessed 25 May 2017

11 See for example, Judgment of Civil Affairs, No. 2976 Year 2014, Taiwan Taipei District Court

12 'Shi Jian Xin You Qiu Bei Google Yi Wang Bai Su' Apple Daily (Taipei, 22 January 2015) <http://www.appledaily.com.tw/apple-daily/article/headline/20150122/36343190/> accessed 25 May 2017

13 'MiYaDu Jia Qiu An Shi Jian Xin Wu Zui Que Ding' Yahoo News (Taipei 22 January 2013) https://tw.news.yahoo.com/%E7%B1%B3%E8%BF%AA%E4%BA%9E%E5%81%87-%E7%90%83%E6%A1%88-%E6%96%BD%E5%BB%BA%E6%96%B0%E7%84%A1%E7%BD%AA%E7%A2%BA%E5%AE%9A-095841449--mlb.html accessed 25 May 2017

THE RIGHT TO BE FORGOTTEN IN TAIWAN, CHINA AND JAPAN

Based on the abovementioned reasoning, the District Court does not consider the defendant as the manager nor sales representative of Google Search engine. In addition, the Court does not reckon Article 184, Article 191-1 of the Civil Code, nor Article 7-9 of the Consumer Protection Act provide a legitimate basis for the plaintiff's claims, on the grounds that the interests safeguarded by the Consumer Protection Act do not cover the right of fame, nor the right to privacy.

Moreover, the plaintiff further requested to add Google Inc. as one of the co-defendants. The claim was first dismissed by the District Court, yet later approved by the Taiwan High Court.[14] The case is therefore now under re-trial at the District Court.

In the abovementioned judgment of Taipei District Court, the reasoning of "the defendant (Google International LLC), who is registered in our country, cannot be deemed as competent and responsible for in managing the Google Search engine, just due to the mere fact that Google Search engine is available for being used in Taiwan", is clearly different from that of CJEU in the *Google Spain* Judgment, where the CJEU gave a much broader interpretation of "establishment" under Article 4 of the Data Protection Directive. However, Taipei District Court was asked by the higher instance to review this case[15] and eventually rendered its judgment in July 2017. In the latest judgment, one can somehow see the influence from the deliberation of the Supreme Court of Japan in January 2017 (which will be introduced below), where more concrete criteria for the internet search engine runner to assess the delisting requests are also introduced and elaborated.

II-DEVELOPMENT IN CHINA

Slightly after the *Google Spain* Judgement, a case in the People's Republic of China also emerged. With more than 700 million netizen in the whole country,[16] how the PRC jurisprudence reacts to the right to be delisted as developed by the CJEU certainly receives great attention. For the purpose of this article, this part of the development of RTBF in PRC will focus only on the most recent case. [17]

The case can essentially be traced back to February, 2015, when the plaintiff, Mr. Ren, started to discover some undesirable search results about himself that appeared on the search engine run by the defendant, Baidu Netcom Science and Technology (Beijing) Co.,Ltd (hereafter: Baidu), which is the biggest internet search engine-runner in China. The search results at issue implied a certain degree of association between the plaintiff and Tao's Education, a training institution located in Wuxi city. According to the plaintiff, Tao's Education has an undesirable reputation, such as being accused of committing fraud.

Mr. Ren works in the field of management training sector with the specialties of human resource management and corporate management. During the trial, Mr. Ren submitted a piece of written evidence of an "Agreement on Dissolving Employment Countract", which showed Mr. Ren and Dao Ya Shuan Commerce & Trade Co.,Ltd "voluntarily" dissolved the employment relationship after consultation, on the ground that after Dao Ya Shuan Commerce & Trade Co.,Ltd retained Mr. Ren, they found out through Baidu search engine that phrases such as "Wuxi Tao's Education Ren XX" were displayed. Since the job that Tao was hired to do requires a high level of credibility, both parties "voluntarily" dissolved the employment relationship because Tao's Education was said to be a "liar company" and even called a "cult" by some people.

Relying on the bases of right to name, right of fame, and the general application of the right to personality, the plaintiff requested Baidu to delete related search results and related links such as "the Tao's Education Ren XX", "Wuxi Tao's Education Ren XX".[18]

In the delivery of the first instance judgment from the Haidian District Court, the Court pointed out the core legal issues of the present case are about the technical model of the "related search" and the legitimacy of this service. The Court further divided its analysis into two parts. The first part concerned the factual judgment on whether the displayed phrases by the "related search" service was artificially intervened in by Baidu, whereas the second part centered on whether the technical model of the "related search" and its corresponding service model had violated the right to name, right of fame, and "the right to be forgotten" in the general application of the right to personality as claimed by the plaintiff.

In terms of the first question, the Court found that

14 Taiwan High Court Ruling 2015 Kang Zi No.491
15 Interim Decision of Civil Affairs, No. 31 Su Geng Yi Year 2017, Taiwan Taipei District Court
16 Statistical Report on Internet Development in China, Chinese Internet Network Information Center, https://cnnic.com.cn/IDR/ReportDownloads/201611/P020161114573409551742.pdf accessed 25 May 2017
17 For a more comprehensive discussion on the possible concept of RTBF in China before prior to 2015, See: Mei Ning Yan, 'Protecting the Right to be Forgotten: Is Mainland China Ready?' [2015] 3 EDPL 190
18 Civil Judgment of People's Court of Haidian District, Beijing, No. (2015)Hai Min Chu 17417

THE RIGHT TO BE FORGOTTEN IN TAIWAN, CHINA AND JAPAN

Baidu had not intervened with the search results as the examination conducted by the Court showed each time the displayed search results vary, corresponding to the testimony of Baidu that these search results are displayed on the basis of the frequency of certain phrases being searched in a defined period of time in the past.

In the second part of the analysis, the Court first concluded that since there is no human intervention in the case, the core question is left to whether the technical model of the "related search" and its corresponding service model had invaded interests as claimed by the plaintiff. In its analysis, the Court first found that six phrases at issue, "Tao's Education Ren XX", "WuXi Education Ren XX", "Tao's Ren XX", "Tao's super learning method", "super fast leaning method", "super learning method", as shown by the Baidu search engine, did not contain any negative connotation, no matter in the format or in the substance. In light of these facts, the Court then accordingly found that there was no infringement to the right of fame, since there was no defamation in the present case. Furthermore, the Court also decided that since there is no misuse of the name, there is no violation to the right of name either.

Most importantly, in deciding whether a general application of right to personality exists, the Court made it clear that since there are no categories of rights such as "the right to be forgotten" in China, it cannot be the lawful source for legal protection. The Haidian District Court further elaborated, that the general application of the right to personality requires a legitimacy test for the interest at issue as well as a necessity test for its protection. The Court then recalled that since Mr. Ren was not a minor nor a person with limited capacity when he cooperated with the Tao's Education, there is no legal foundation for the exceptional protection. Accordingly, the Court decided that there is no legitimacy nor necessity for legal protection for the interests "to be forgotten"(to be deleted) as claimed by the plaintiff. After six months, the second instance court upheld the decision by the Haidian Distrct Court, without much alteration of its reasoning.

III-INFLUENCES ON JAPAN

In addition to Mandarin-speaking jurisdictions such as Taiwan and China, several cases related to the right to be forgotten also appeared in Japan between 2014 and 2015. As Professor Shizuo Fujiwara rightly noted in his analysis published on the e-conference of blogdroiteuropeen, one of the most exciting developments in 2017 is that the Supreme Court of Japan completed its review in January on the original judgment of No. 17 from Saitama District Court in June 27, 2015.

The plaintiff of this case was arrested for having prostitution offered by a minor in exchange for remuneration.[19] In 2012, the plaintiff found out that 49 search results related to the abovementioned event, would show up after typing in the plaintiff's address and name in the Google search. Therefore, the plaintiff filed the claim against the Google Inc. in the U.S.A., which administer and run the Google search website, requesting it to delete those search results on the grounds of protecting the personality right of those who had a criminal history and are going through the rehabilitation process.

To counter the plaintiff's claim, Google has argued the same reason that it provided in the *Google Spain* Judgment, that the search results are the outcomes of processing of algorithms by a computer, which is without human intervention. In addition, Google pointed out that the present case involved information regarding prostitution offered by a minor in exchange for remuneration, which fell into the category of information with significant public interest. The revealing of this information should thus be within the limit of minor invasion towards the plaintiff's right.

For its deliberations, the Saitama District Court first considered the meaning and necessity of revealing the plaintiff's record of being arrested in the search results. In its assessment, the District Court pointed out that having prostitution offered by a minor in exchange for remuneration is a severely criticized crime, both in Japan and internationally. In light of the considerations of future possible victims as well as their parents, and the concerns of the society on this issue, it is undoubtedly beneficial to the general "right to know" of the society and thus is of public interest. The court further mentioned that, however, what is not shown in the search results, is that the plaintiff was sentenced to a 50,000 yen fine and lives peacefully with his wife. Furthermore, how the story happened and how it later unfolded was not shown in the search results, but only the record of plaintiff's being arrested and related reportage.

The Saitama District Court thus reckoned that the plaintiff was entitled to his request. Nevertheless, the High Court of Tokyo later overruled the judgment of the Saitama District Court, in the belief that the removal of the search results will compromise freedom of speech as well as the right to know. [20]

19 According to Article 2 of the Japanese *Act on Regulation and Punishment of Acts Relating to Child Prostitution and Child Pornography, and the Protection of Children*, the term «child» used in this Act shall mean a person under 18 years of age.
20 Wasurarerukenri"Mitomezu kensukukekkano Suku-

THE RIGHT TO BE FORGOTTEN IN TAIWAN, CHINA AND JAPAN

Moreover, the Supreme Court of Japan upheld the decision of the High Court of Tokyo. In its deliberation on 31st January, 2017, the Supreme Court of Japan further provided the criteria for the search engine runner to assess upon receiving the request of the data subject regarding the removal of certain content in the search results, if these results disclose things such as reportages that covers facts belonging to the privacy of the requester. The criteria have been noted by Professor Shizuo Fujiwara in his contribution, "Current situation of discussions on Right to be forgotten in Japan", published in this collection.

IV-CONCLUDING OBSERVATIONS

As many previous presenters of the e-conference have noted, the development of the RTBF in the past 20 years, has evolved from the very early discussions in the nineties, to the early legal design in the 2012 GDPR proposal, to the 2014 *Google Spain* Judgment, and eventually, to the present impacts that have unfolded all over the world.

In terms of the representative cases chosen in this article, interesting ramification are observed from positions chosen by the judicial agencies in non-EU zones. In Taiwan, despite the reference quoted towards both the *Google Spain* Judgment and the Japanese RTBF case, the Taipei District Court has chosen to bypass the issue by the façade of using formalities criteria blocking substantial deliberations of the case. In China, on the contrary, the Courts (both the first and second instance) clearly expressed their decisions that the RTBF, for the Chinese judiciary, is yet only a right recognized by the EU, and there will hardly be any protection offered if one bases his or her claim solely on this "interest". Last but not the least, RTBF was firstly recognized by the confirmation of a lower court in Japan, but eventually denied by the Supreme Court of Japan, who did not use the wording of RTBF but provided a set of concrete criteria for the internet engine search runner to weigh against the requests of deletion of certain search results from the users, when the facts at issue are related to privacy.

As presented in the *Google Spain* Judgment, and later cases all over the globe, the conflicts that emerge in those cases of "the right to be delisted" are among freedom of speech, right to information from the public on the one hand, and personality rights, values of privacy and data protection on the other side. Interestingly, for the failure of resorting to the RTBF in China, one might see it as a result of the absence of discourse on the privacy violation, as compared to the case in Japan. Furthermore, from all of the three cases chosen, it can be observed that despite the impacts that have arisen from the *Google Spain* Judgment, the value of privacy that varies locally so far still has greater influence on jurisdictions outside Europe concerning the development of RTBF.

In the age of big data, facilitated by the trends of Internet of Things, unprecedented data is being produced every second, of which a great deal is related to identifiable individuals. From the perspective of informational autonomy, individuals' right to control their own data shall be undoubtedly recognized. This should be a universal scenario.

As Viktor Mayer-Schönberger pointed out in his famous article, *Delete: The Virtue of Forgetting in the Digital Age*, in the digitalized age, forgetting has become an exception to memorizing. As the cases suggest, the assessment of each case on the right to be forgotten relies significantly on *ad hoc* evaluations. As a matter of fact, the RTBF is still developing both within and outside of the EU, namely in the 2017 CJEU judgment on Lecce or the case that still awaits the reconsideration by the district court in Taiwan. However, in terms of legal certainty and its impact on the search engine business runner or internet archivers all over the world, a set of more predictable (and perhaps simpler) criteria for both the enterprises and the court, are still needed to strike a balance between the eternal memories of the internet and the human need for privacy.

joyouseiwokyakka Tokyokousai' *The Japan Newspaper Publishers & Editors Association* (Tokyo, 28 July 2016) <http://www.press-net.or.jp/news/headline/160712_10268.html> accessed 25 May 2017

ANNEX 1 : CONCLUSIONS DE MME LA RAPPORTEURE PUBLIC AURÉLIE BRETONNEAU

399922 – GOOGLE INC.

Par une décision du 24 février 2017 (CE, Assemblée, 24 février 2017, Mme C. et autres, n°s 391000 393769 399999 401258, p.), l'Assemblée du contentieux a battu un record en posant à la Cour de justice de l'Union européenne (CJUE), à propos de son arrêt Google Spain (CJUE, Grande chambre, Google Spain SL et Google Inc. contre Agencia espanola de proteccion de los datos et Mario Costeja Gonzalez, aff. C-131/12), pas moins de huit questions préjudicielles. Nous allons vous proposer d'en ajouter quelques unes à la liste.

L'arrêt Google Spain est celui par lequel la CJUE a déduit de la directive du 24 octobre 1995 sur le traitement des données à caractère personnel[1] un droit improprement surnommé « à l'oubli », qui est en réalité un droit des individus à obtenir que, quand on tape leur nom sur un moteur de recherche en ligne, certains résultats ne sortent pas.

Vous vous souvenez que cet arrêt procède d'une triple audace. La première audace est d'avoir attrait l'activité exercée par la société mère Google Inc. depuis les Etats-Unis dans le champ d'application territorial de la directive, en s'attachant à la présence en Europe de filiales publicitaires. La deuxième audace est d'avoir qualifié les exploitants de moteurs de recherche de responsables de traitement au sens de la directive, alors même qu'ils n'ont pas de prise directe sur les données que le moteur indexe à partir de pages publiées et hébergées par d'autres sur Internet. La troisième audace est d'avoir dégagé, à partir de dispositions de la directive qui n'ont pas, compte tenu de leur âge, pu être écrites pour cela, un droit au déréférencement paramétré de façon prétorienne. Elle a ainsi permis à toute personne privée d'exiger d'un moteur qu'il supprime de la liste des résultats affichés à la suite d'une recherche effectuée à partir de son nom et prénom les liens vers des pages web contenant des informations la concernant, chaque fois que le surcroît de publicité induit par leur référencement porte à sa vie privée une atteinte disproportionnée à la finalité du traitement. Autrement dit, la CJUE a tiré d'une directive antérieure à la création de Google Inc. une obligation pour cette société d'effacer le chemin qui, du fait du moteur qu'elle exploite, relie certaines données au nom de la personne. Le tout au terme d'une balance entre intérêt du référencement de l'information pour le public et atteinte à la vie privée née de cette facilité de consultation.

Vous vous souvenez aussi que cette création prétorienne pose deux difficultés.

La première difficulté, au cœur des affaires portées en Assemblée, concerne la portée matérielle du droit créé. L'affirmation de l'arrêt Google Spain selon laquelle la balance entre intérêt du public et respect de la vie privée vaut « même lorsque le traitement des données par le site source est licite » pose des problèmes d'a contrario, et rend incertaine la conduite à tenir face à des données dont le jeu mécanique de la directive interdit purement et simplement le traitement. C'est pourquoi vous avez renvoyé à la CJUE le soin de dire pour droit si la qualification de responsable de traitement emporte pour les moteurs de recherche l'interdiction de référencer les données relatives à la vie sexuelle, aux opinions ou aux condamnations pénales, y compris lorsque leur intérêt pour le public est avéré.

La seconde difficulté, au cœur de la présente affaire, se situe en aval et concerne le champ non plus matériel, mais géographique du droit au déréférencement. Elle consiste à savoir si, lorsqu'un moteur de recherche est tenu de déréférencer, il doit le faire uniquement dans la zone géographique couverte par la directive, ou s'il doit, compte tenu de l'indifférence d'internet aux frontières, y procéder partout, moyennant une forte dose d'extraterritorialité. Subsidiairement, se pose la question de la bonne façon de procéder à une limitation géographique du champ du déréférencement. Concrètement, il faut décider si Google Inc. doit effacer le chemin entre nom de la personne et informations en ligne sur l'ensemble des terminaisons du moteur y compris mondiales (.com) ou uniquement sur ses terminaisons nationales et/ou européennes (.fr, etc.), à moins qu'il ne s'agisse de mettre en place un système de « géoblocage » interdisant l'accès aux données déréférencées depuis le sol européen.

Nous allons revenir sur les implications techniques et juridiques de ces formules. Mais nous voudrions d'abord faire trois séries d'observations.

Premièrement, nous employons à dessein le lexique de la géographie, parce qu'il est le plus parlant pour décrire les questions posées. Mais ce vocabulaire est impropre, car il n'est pas de géographie qui tienne sur internet, où n'existent que des ersatz de frontières imparfaitement imitées. C'est dire l'ampleur de la problématique centrale du litige, celle de

1 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

ANNEX 1 : CONCLUSIONS DE MME LA RAPPORTEURE PUBLIC AURÉLIE BRETONNEAU

l'adaptation des matrices juridiques traditionnelles, reposant sur une forte territorialisation du droit, à l'a-territorialité propre à l'outil numérique.

Deuxièmement, la question du champ territorial du déréférencement, distincte de celle de son champ matériel, entre en résonnance avec elle. Plus le droit au déréférencement sera largement reconnu, sur la base de critères spécifiques à la législation de l'Union européenne, plus son extension géographique au-delà des frontières virtuelles de l'Europe se posera en termes de choc des cultures et des conceptions. En outre, dès lors que l'arrêt Google Spain impose de mettre en balance l'atteinte à la vie privée avec l'intérêt du public à accéder à l'information litigieuse, il faut bien s'entendre sur le public cible de l'information.

Troisièmement, les deux difficultés relatives au champ, matériel et territorial, du déréférencement, sont elles-mêmes intimement liées aux trois audaces dont procède la création prétorienne de la Cour. En attrayant de façon volontariste les moteurs de recherche dans le champ territorial de la directive, la CJUE a entendu faire échec à l'immunité que rendait possible la faculté de déployer une activité dans le monde entier sans avoir à se soumettre, faute de contrainte de localisation, aux règles voulues par les Etats à l'intérieur de leurs frontières. En assimilant à toute force les moteurs de recherche à des responsables de traitement, et en tirant de l'effet d'amplification des informations propres à ces moteurs une obligation sui generis de mettre un terme à cet écho, la CJUE a trouvé une martingale juridique à l'effet « ubiquitaire »[2] d'internet. Il s'ensuit que la question qui vous est posée n'est pas celle d'une banale modalité pratique d'exercice du droit au déréférencement, mais celle d'un élément clef de son paramétrage.

Ces précisions étant faites, venons-en au litige qui sert d'écrin à cette délicate question.

La Commission nationale informatique et libertés (CNIL), chargée d'assurer sur le fondement de la loi n° 78-17 du 6 janvier 1978 l'application en France du droit au déréférencement, a observé les pratiques de la société Google Inc., débitrice de l'obligation de déréférencer. Elle a constaté que la société, lorsqu'elle faisait droit à une demande de déréférencement, n'y procédait pas sur l'ensemble des extensions de noms de domaine de son moteur de recherche, et en particulier pas sur l'extension .com. Estimant que cette pratique n'était pas de nature à assurer de façon effective la protection voulue par l'arrêt Google Spain, la présidente de la CNIL a, le 21 mai 2015, mis la société en demeure d'appliquer le déréférencement à toutes les extensions de noms de domaine du moteur. La société Google Inc. ne s'étant pas conformée à cette obligation, la formation restreinte de la CNIL lui a, par la délibération litigieuse du 10 mars 2016, infligé une sanction pécuniaire rendue publique de 100 000 euros.

De la procédure d'instruction de cette sanction et du litige de plein contentieux dont vous êtes saisis résulte l'existence d'une opposition frontale quant à la portée du droit au déréférencement entre la CNIL, dans le sens de laquelle le défenseur des droits a présenté des observations, et la société Google Inc., soutenue par six interventions recevables rassemblant quarante-et-un intervenants.

Pour la CNIL, le droit au déréférencement est avant tout une garantie visant à assurer aux bénéficiaires de la directive, c'est-à-dire aux personnes privées résidant sur le sol européen, une protection contre l'effet démultiplicateur qu'ont les moteurs de recherche sur la notoriété des informations personnelles en ligne. Il confère donc à ses bénéficiaires un droit à ce qu'aucune personne qui s'aviserait de « googliser »[3] leur nom ne trouve ce faisant certaines informations. Dans la mesure où n'importe qui peut les « googliser » de n'importe où, le déréférencement doit, pour ne pas manquer son but, revêtir un caractère global. Dans cette conception, le droit au déréférencement est attaché à la personne et se trouve lésé dès lors qu'un tiers a accès, en réponse à une recherche à partir de son nom, aux informations litigieuses. Dans cette conception, le lieu de consultation importe peu et le caractère ubiquitaire de la mise en ligne emporte le caractère universel du déréférencement. La CNIL résume cette conception en convoquant l'image d'une « bulle juridique » qui enserre le titulaire du droit au déréférencement et suit ses données personnelles partout où elles peuvent être consultées.

Pour la société Google Inc., le droit au déréférencement est avant tout une modalité contraignante d'exercice du traitement par l'opérateur, qui ne le saisit qu'en tant qu'il tombe dans le champ d'application, notamment territorial, de la directive. Dans cette optique, le droit au déréférencement, qui s'applique à l'affichage des résultats par le moteur de recherche exploité dans le cadre des activités d'un établissement stable implanté sur le sol de l'Union européenne, ne joue qu'en tant que ces résultats s'affichent sur le territoire européen. Aux antipodes de la bulle mobile décrite par la CNIL, le droit au déréférencement s'apparente plutôt, pour la société Google Inc., à une cloche protégeant fixement le territoire européen et lui seul, les informations personnelles pouvant continuer d'être traitées librement sur internet en dehors de son champ.

2 Le terme est employé par la Cour dans l'arrêt Google Spain, §80.
3 Néologisme qui a fait son entrée dans l'édition 2015 du Petit Larousse et dans l'édition 2018 du Robert (il y est précisé qu'on dit aussi « googler »).

ANNEX 1 : CONCLUSIONS DE MME LA RAPPORTEURE PUBLIC AURÉLIE BRETONNEAU

Ce débat principal se double à titre subsidiaire d'une controverse sur la possibilité de circonscrire géographiquement le déréférencement. Pour la CNIL, quand bien même il ne faudrait assurer la confidentialité des données personnelles qu'en Europe, les solutions techniques proposées par Google pour assurer ce paramétrage fin sont facilement contournables, de sorte que seul un déréférencement global peut garantir une mise sous cloche effective du territoire européen.

Pour vous convaincre de ce que sa conception est la bonne, la société et les intervenants soulèvent trois moyens principaux : la portée extraterritoriale que donne la CNIL au droit au déréférencement méconnaît les principes élémentaires du droit international ; elle porte une atteinte disproportionnée à la liberté d'expression ; et la délibération se trompe en estimant que les solutions de circonscription territoriale proposées n'assurent pas la protection des droits fondamentaux.

Mais en amont de cette contestation de fond, la société soutient aussi que la formation restreinte de la CNIL était incompétente pour sanctionner le fonctionnement de google search au-delà du fonctionnement de google.fr. La question est un peu de guingois car ce que la formation restreinte sanctionne, c'est la méconnaissance de la mise en demeure, ce qu'elle est nécessairement compétente pour faire. Mais on comprend l'idée, qui est que la CNIL ne peut, en termes de compétence, se mêler d'autre chose que du fonctionnement de google.fr, que Google Inc. assimile au volet français de google search, ce dernier ne pouvant être saisi globalement. Google Inc. avance deux arguments.

Un premier argument, fondé sur la circonstance que le traitement serait partiellement mis en œuvre hors du territoire national que la CNIL est compétente pour réguler, s'écarte facilement. La compétence de la formation restreinte s'apprécie en deux étapes. D'abord, il faut que l'opérateur soit saisi par le champ d'application de la loi, faute de quoi il n'y a pas de manquement. C'est le cas de la société Google Inc. puisque, comme vous l'avez jugé, l'article 5 de la loi transpose au territoire français l'article 4 de la directive, qui saisit l'activité d'ensemble du moteur dès lors qu'il a sur le territoire un établissement publicitaire – sa filiale Google France. Cette étape franchie, l'article 48 de la loi, transposant l'article 24 de la directive, prévoit que le pouvoir de sanction s'exerce « à l'égard des traitements dont les opérations sont mises en œuvre, en tout ou partie, sur le territoire national ». Il en résulte que la CNIL est compétente pour connaître des manquements à la loi commis par les opérateurs à raison des traitements qu'ils exploitent dans le cadre d'un établissement situé en France, y compris lorsque les opérations du traitement ne sont que partiellement mises en œuvre sur le territoire national.

Plus délicat est le second argument, tiré de ce que l'activité du moteur de recherche google search ne serait pas constitutive d'un traitement unique, mais d'une multiplicité de traitements distincts. En particulier, constituerait un traitement à part entière l'affichage de résultats sur le nom de domaine google.fr, qui seul tomberait dans l'escarcelle de la législation française. Restituer l'argumentation implique de retracer les opérations techniques qui se cachent derrière l'instant magique où, ayant tapé un mot clef sur Google, l'internaute obtient en un clic toute les réponses aux questions existentielles qu'il s'était toujours posées.

Comme l'a expliqué la société Google Inc. à la 10ème chambre lors de l'audience d'instruction qui s'est tenue le 9 novembre 2016, le fonctionnement du moteur de recherche est comparable à celui d'une bibliothèque en ligne que viendraient consulter les internautes.

La première étape consiste, comme pour la constitution du fond d'ouvrages d'une bibliothèque, à récolter des données, en l'occurrence des pages web. La collecte est réalisé par la fonction d'exploration googlebot à l'aide de robots, appelés web-crawlers, qui parcourent internet pour en inventorier le contenu. Les données sont stockées dans des centres de données, qui constituent des bases identiques et mises à jour en continu. La deuxième étape consiste pour le moteur, à l'instar du bibliothécaire qui cote les ouvrages et y associe des notices bibliographiques, à « indexer » les pages répertoriées, c'est-à-dire y associer des meta-données, telles que la langue de rédaction ou le page rank, sorte d'indice de qualité intrinsèque attribué par Google à la page concernée. Ces deux opérations débouchent sur une base de données indexées unique dans laquelle le moteur de recherche puisera pour répondre aux requêtes.

C'est alors qu'intervient la requête de l'internaute. Pour la traiter, le moteur procède à nouveau en deux temps.

Le premier temps est celui où, à l'instar du bon bibliothécaire, il cherche à en savoir plus sur les besoins de l'usager pour améliorer la pertinence des résultats qu'il s'apprête à lui proposer. Parmi les informations qu'il récolte figure en bonne place le domaine sur lequel l'internaute effectue sa recherche. Google a en effet fait le choix de déployer son moteur de recherche, outre sur google.com, sur plusieurs extensions, correspondant peu ou prou à des déclinaisons nationales – il en existe environ 200, dont google.fr. De l'extension choisie, Google infère une probabilité de lien avec la zone géographique concernée. Cette information est croisée avec d'autres, telles que l'adresse IP, c'est-à-dire l'adresse physique du terminal informatique à partir duquel est effectuée la recherche, qui elle aussi renseigne sur les accointances géographiques du demandeur, voire avec des coordonnées GPS dans les cas où une fonctionnalité de ce type est actionnée par l'internaute. La langue de recherche est également mobilisée. Et en plus de ces informations recueillies pour tous les internautes, Google en

obtient d'autres pour les utilisateurs dont le compte gmail, qui regorge d'informations, est ouvert lors de la recherche. Ces informations sont utilisées pour constituer une pré-liste de résultats corrigée des incertitudes pouvant résulter des mots-clefs choisis par l'internaute. Ainsi, la saisie du mot « football » ne donnera pas la même pré-liste selon que l'internaute est réputé français ou localisé dans un pays de langue anglaise, où ce vocable désigne le football américain. Le mot « papillon » ne sera pas interprété de la même manière selon que le compte Google révèle un intérêt pour la nage ou pour l'entomologie.

Le dernier temps est celui de l'affichage des résultats. Il consiste à appliquer des filtres à la pré-liste de résultats pour ajouter ou retrancher des informations. Le principal ajout est celui de la publicité. Les retranchements sont fonctions d'obligations légales : sont dissimulés les résultats interdits par les législations sur la pédopornographie, le terrorisme, les droits d'auteurs, ainsi que par les régimes de censure locale. C'est également à ce stade qu'est appliqué le déréférencement (contrairement à la désindexation, qui consiste à retirer les liens de la base de données).

De ce séquençage technique Google Inc. déduit d'abord que chacune des quatre étapes – collecte, indexation, constitution de la pré-liste, affichage – constitue un traitement à part entière. Elle considère en outre que, dès lors que l'affichage varie selon les noms de domaine, alors chaque terminaison nationale (google.fr, google.uk, etc.) constitue un traitement distinct, lui-même distinct de google.com. Elle conclut que, dès lors que l'arrêt Google Spain ne concerne que l'affichage – du fait à la fois de l'accroche par la filiale publicitaire dont l'activité se déploie à cette étape et du stade d'intervention du déréférencement – alors il ne concerne que l'affichage sur les traitements autonomes que sont les extensions européennes, la CNIL n'étant compétente que pour le faire respecter sur l'extension française.

Cet argumentaire, même affaibli par la circonstance que Google a souscrit pour l'ensemble de l'activité de son moteur une déclaration unique auprès de la CNIL, ne manque pas de force. Mais, à la réflexion, il ne nous convainc pas.

Premièrement, la circonstance que l'activité du moteur se subdivise en plusieurs opérations techniques distinctes ne suffit pas à emporter la qualification de traitements distincts. Les articles 2 de la directive et de loi informatique et libertés qualifient ainsi de traitement, au singulier, « toute opération ou ensemble d'opérations » telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction des données. L'arrêt Google Spain juge expressément que « l'activité d'un moteur de recherche consistant à trouver des informations (…) sur internet (…), à les indexer de manière automatique, à les stocker temporairement et, enfin, à les mettre à la disposition des internautes selon un ordre de préférence donné doit être qualifiée de traitement [au singulier] de données à caractère personnel ». Nous ne croyons donc pas au séquençage par tranches d'opérations.

Ce pas étant franchi, nous ne croyons pas non plus au séquençage par noms de domaine.

Au plan technique, le lien qu'opère Google Inc. entre le caractère différent de l'affichage selon les noms de domaine et le fait que chaque nom de domaine constitue un traitement en propre n'est pas très convaincant. On l'a vu, la différenciation des résultats, processus qui s'enclenche au stade de la constitution de la pré-liste, dépend d'une multiplicité de facteurs parmi lesquels le nom de domaine ne joue qu'un rôle marginal, de sorte que s'il fallait compter autant de traitements que d'affichages, alors il y aurait autant de traitement que d'internautes, voire de requêtes. D'ailleurs, si l'affichage peut varier en fonction des noms de domaine, tel n'est pas systématiquement le cas : exemple emblématique, l'activité publicitaire déployée au stade de l'affichage l'est sur la base de l'adresse IP[4] : résultat, la publicité gérée par Google France s'affiche dès lors que la recherche est réputée lancée depuis le territoire français, quelle que soit la version du site (.fr, .com., ou autre) que l'internaute utilise.

En outre, il existe des passerelles entre les différentes déclinaisons du moteur, qui affaiblissent l'idée de traitements développés distinctement. Ainsi, un internaute effectuant une recherche sur l'extension google.com est automatiquement redirigé, en fonction de l'adresse IP de son terminal, vers le nom de domaine national correspondant. Lorsqu'un internaute dont le compte gmail est actif effectue une recherche sur un domaine A, celle-ci, stockée dans les informations de son compte, sera prise en compte, au titre de l'historique de ses recherches, pour affiner la pertinence des résultats y compris pour des recherches ultérieures sur un domaine B. Enfin, lors de l'audience d'instruction, la CNIL a apporté la démonstration qu'un cookie (sorte de micro-fichier permettant de conserver des données de l'utilisateur afin de faciliter la navigation et de permettre certaines fonctionnalités) issu de google.com pouvait, même sans compte gmail actif, être déposé à l'occasion d'une recherche sur google.fr. Même si Google Inc. soutient que cette faculté n'est ouverte qu'à des cookies techniques, elle témoigne de la porosité entre les différentes versions de google search. Conjuguée au fait que toutes ces versions puisent à la source de la même banque de données indexées, cette porosité accrédite l'idée d'un traitement d'ensemble.

4 Pour Internet Protocol : il s'agit du numéro d'identification qui est attribué à chaque appareil connecté à un réseau informatique utilisant l'Internet Protocol – en quelque sorte l'adresse physique du terminal informatique connecté au réseau.

ANNEX 1 : CONCLUSIONS DE MME LA RAPPORTEURE PUBLIC AURÉLIE BRETONNEAU

Au plan juridique, la qualification de traitements distincts n'apparaît de toute façon pas déterminante : le critère de compétence est celui des traitements déployés dans le cadre de l'activité de la filiale française mis en œuvre au moins en partie sur le territoire français. Or s'il est vrai que découpage des domaines se veut une réplique virtuelle du périmètre des Etats (imparfaite : l'Outre-mer n'est pas couvert par le .fr), l'ensemble des versions dites nationales est accessible depuis la France, l'internaute ayant le choix de refuser la redirection automatique pour effectuer ses recherche en .com ou sur n'importe laquelle des autres extensions de google search. Serait-elle déterminante qu'elle aurait le curieux effet de faire dépendre la prise du régulateur sur un moteur de recherche du choix contingent de l'exploitant de le décliner ou non en terminaisons nationales. La CNIL se retrouverait compétente pour connaître de l'activité unique d'un moteur fonctionnant uniquement en .com, tandis que Google Inc. échapperait largement à sa juridiction grâce au choix, qui n'est d'ailleurs pas d'origine, de décliner désormais son moteur en version nationales. Sans compter que ce tronçonnage en traitements distincts par terminaisons nationales miroiterait avec la logique de l'arrêt Google Spain, qui est plutôt de partir du caractère ubiquitaire de l'activité de Google Inc. pour la saisir en dépit des matrices traditionnelles de la territorialité.

Nous sommes donc d'avis de regarder google search comme un traitement unique doté de multiples chemins d'accès techniques et d'écarter le moyen tiré de ce que la CNIL serait incompétente pour connaître de l'activité de l'ensemble des traitements distincts, ainsi que les moyens d'insuffisance de motivation et d'erreurs de droit, de qualification juridique et de fait à avoir, dans la délibération litigieuse, retenu cette qualification.

Vous pourriez hésiter à faire cette réponse vous-mêmes plutôt que d'en laisser le soin à la CJUE, dans la mesure où lui renverrez selon nous le reste des questions posées par le litige. Mais d'une part, vous ne devez poser à la Cour que les questions d'interprétation de la directive qui présentent une difficulté sérieuse : or il nous semble assez clair, compte tenu des termes de la directive éclairée par l'arrêt Google Spain, que la notion de traitement conduit à appréhender google search dans son ensemble. D'autre part, la qualification de traitement unique ne préempte pas le sort des autres moyens car, si elle rend possible la prescription d'un déréférencement global, elle ne l'induit pas techniquement et n'exclut pas de la regarder juridiquement comme illégitime ou disproportionnée.

*

Venons-en à ces moyens de fond, dont l'exposé suffit à témoigner des enjeux quasi-philosophiques qui expliquent l'attention que la doctrine et les médias portent à la question technique de la portée territoriale du droit au déréférencement.

Le premier est tiré de ce que la portée extraterritoriale que donne la CNIL à ce droit méconnaît les principes du droit international public de souveraineté nationale, de courtoisie et de respect des décisions de justice étrangères. La société part du constat que plusieurs juridictions d'Etats tiers, notamment en Colombie et au Japon, se sont explicitement prononcées en défaveur d'un droit au déréférencement. Elle relève à l'inverse que, dans les Etats tiers où un droit au déréférencement existe, il n'a pas la même consistance qu'à l'intérieur de l'Union : elle prend l'exemple de la Russie, où ce droit, y compris lorsqu'il concerne les personnalités publiques, s'exerce en dépit de l'intérêt pour le public d'accéder à l'information. Elle en déduit que, si chaque Etat qui consacre un droit au déréférencement prétend à l'universalité de sa mise en œuvre, alors son choix percutera nécessairement celui fait par d'autres Etats de ne pas restreindre l'accès à l'information dans sa juridiction, et conduira en outre à aligner l'internet sur le standard le plus restrictif, puisque tous les internautes subiront l'effacement des résultats voulus par le plus sévère des régimes. Le risque est d'autant plus sensible qu'en temps normal, les conflits de législations dus à l'extraterritorialité butent sur l'incapacité de l'Etat source à obtenir l'exécution des prescriptions sur le sol d'un autre Etat. Mais compte tenu de l'extraterritorialité d'internet, l'exécution d'un déréférencement global obtenue en France a des effets immédiats dans le monde entier.

Ici, la prise contentieuse et l'opérance même du moyen dépendent de la question de savoir si le déréférencement global auquel sont faits ces reproches découle d'une lubie de la CNIL ou bien directement de la directive telle qu'interprétée par la décision Google Spain et transposée par la loi française. En tout état de cause, son traitement impliquerait une pesée en termes de proportionnalité, l'un des plateaux de la balance étant lesté différemment selon que l'efficacité d'un droit garanti par la Charte est conditionné ou non au déréférencement global.

Le deuxième moyen est tiré de ce que l'exigence de déréférencement global porte aux libertés d'expression, d'information, de communication et de la presse une atteinte disproportionnée, en imposant de masquer des informations y compris en dehors du territoire où s'applique la protection de la vie privée qui justifie cet effacement.

Pour l'appréhender justement, il faut, au risque de briser l'image d'Epinal selon laquelle internet est l'espace de la liberté la plus complète et les autorités de régulation les bras armés de la censure, préciser que ces libertés ne sont qu'indirectement en cause. En premier lieu, parce que le déréférencement de données personnelles n'entraîne jamais leur disparition d'internet. Ces données demeurent sur le site source qui les a publiées, qui continue d'être accessible soit par

saisie de son adresse URL[5] dans la barre d'adresse du navigateur, soit via le moteur de recherche, par la saisie d'autres mots-clefs pertinents que le nom et le prénom de la personne concernée. En second lieu, parce nous ne croyons pas à la présentation selon laquelle internet, tel qu'on y accède par le prisme d'un moteur de recherche, serait un lieu de consultation pur et parfait de l'information en ligne. Comme tout exploitant de moteur de recherche, la société Google Inc. organise, via l'algorithme qui est un des secrets commerciaux les mieux gardés au monde, une hiérarchisation des résultats par mots-clefs qui poursuit un objectif commercial dont il n'y a pas à rougir, mais qui n'a rien de neutre et n'offre pas aux auteurs de contenu un droit au référencement sur lequel reposerait toute entière leur liberté d'expression. Si ces libertés sont en cause, c'est donc uniquement en tant que l'indexation par un moteur de recherche contribue potentiellement à la bonne diffusion des informations, laquelle participe marginalement de la liberté de communication et donc d'expression (v. Cons. const., 10 juin 2009, déc. nº 2009-580 DC ; côté conventionnel, v. not. CEDH, Autronic AG v. Switzerland, 22 mai 1990, 12726/87 : CEDH, 18 mars 2013, Yildrim c/ Turquie, n° 3111/10).

Le moyen est donc opérant. Mais son traitement dépend tout entier de la question de savoir si le déréférencement global est ou non impliqué par l'arrêt Google Spain. Dans la mesure où la directive entend seule régir la conciliation entre protection des données personnelles et libertés des responsables de traitement, on voit mal en effet que vous puissiez estimer proportionnée à l'objectif de protection une obligation de déréférencement global excédant largement, le cas échéant, les restrictions à l'activité des opérateurs qu'a entendu poser la directive. Inversement, il va de soi qu'il ne vous reviendrait pas de juger disproportionnée à l'objectif de protection des droits une mesure découlant directement de la directive.

Or il est rien moins qu'évident de trancher entre la position de la CNIL et celle de Google Inc., l'arrêt Google Spain étant muet sur la question.

Au soutien de sa position selon laquelle le droit au déréférencement ne peut être plus qu'un droit à la dissimulation de certains résultats de recherche sur le sol européen, Google Inc. tire argument du critère qui fonde l'application de la directive dont la CJUE a dégagé ce droit. Cette directive a vocation à régir l'activité des opérateurs dont le traitement est au moins en partie déployé sur le sol européen, au motif de ce déploiement sur le sol européen. En conséquence, les restrictions à l'activité des responsables de traitement qui en découlent ne peuvent pas déborder la ratio legis de cette accroche géographique. Et si la directive consacre pour les responsables de traitement un devoir de dissocier certaines données du nom des personnes qui en font la demande au titre de leur vie privée, ce n'est qu'en tant que le référencement porte atteinte à la vie privée le territoire européen que ce déréférencement peut être imposé à titre de correctif.

Cet argument ne peut s'écarter d'un revers de main. Mais pour le contrebattre, la CNIL s'appuie sur de solides arguments issus de la logique de l'arrêt Google Spain. Pour la CNIL en effet, l'arrêt Google Spain part du principe que la directive ne fait qu'organiser une modalité de mise en œuvre des droits fondamentaux que la Charte des droits fondamentaux de l'Union attache aux personnes. Dès lors, à partir de l'instant où un responsable de traitement se trouve attrait dans le champ d'application de la directive, il lui incombe d'assurer le respect plein et entier de ce droit par son traitement, en mobilisant le cas échéant le déréférencement. La Charte ne garantissant pas aux personnes un droit superficiel à ne pas voir que leurs données personnelles sont traitées, mais un droit substantiel à ce que les internautes, quels qu'ils soient, ne les trouvent pas en tapant leur nom, le déréférencement ne peut être que global. Or force est de constater que la Charte a bien pour clef d'entrée les bénéficiaires du droit (« Toute personne a droit à la protection des données à caractère personnel la concernant »), et que l'arrêt Google Spain tire son volontarisme assumé du fait que la directive a pour objet de maximiser la protection offerte par la Charte (v. les points 58, 66 et 68, citant les jurisprudences Connolly/Commission, C-274/99 P, EU:C:2001:127, Österreichischer Rundfunk e.a., EU:C:2003:294, IPI, EU:C:2013:715, et Rijkeboer, C-553/07, EU:C:2009:293, point 47). Le nouveau règlement général sur la protection des données, adopté dans le sillage de Google Spain le 27 avril 2016, qui prévoit l'application des règles européennes à « tout traitement de données relatif à des personnes se trouvant sur le territoire de l'Union ou lié à l'offre de bien et de services à ces personnes ou au suivi de leur comportement », conforte rétrospectivement cette approche.

Les commentateurs n'ont d'ailleurs pas attendu la position de la CNIL pour souligner la dimension potentiellement hégémonique de l'arrêt Google Spain, d'autant plus qu'une certaine incertitude entoure l'étendue des bénéficiaires du droit au déréférencement : dans ses lignes directrices, le G29 qui rassemble les autorités de régulation européenne affirme que « selon le droit de l'UE tout le monde a droit au respect de ses données personnelles. En pratique, les autorités nationales de protection se concentreront sur les plaintes qui ont un lien clair avec l'Union européenne, par exemple lorsque la personne concernée est un citoyen ou un résident d'un État membre de l'UE » Certains auteurs ont estimé cette formulation assez vague pour inclure non seulement les résidents de passage, mais tout ressortissant d'un pays tiers qui utiliserait une version européenne du moteur de recherche, utilisation qui pourrait être guidée uniquement par l'objectif d'actionner par ce biais

5 Uniforme Resource Locator.

un déréférencement global. Ils en déduisent que si l'arrêt Google Spain imposait un déréférencement global, celui-ci devrait au moins céder ponctuellement face aux droits concurrents dont pourraient être titulaires les personnes n'ayant pas de lien avec l'Union, par exemple leur droit d'accès à l'information.

En l'absence de tout indice quant à la teneur du droit et à ses limitations éventuelles, il n'appartient qu'à la CJUE, qui l'a créé par voie prétorienne, de répondre à ces questions.

Ce d'autant que si vous estimiez pouvoir opter vous-mêmes pour la moins hardie des réponses – celle du déréférencement local – vous ne seriez pas tirés d'affaire pour autant. La CNIL estime en effet que même cet objectif de second rang n'est pas atteint de façon satisfaisante par la façon de faire de la société Google Inc. C'est la raison d'être du dernier moyen de la société, tiré de ce que la délibération est entachée d'erreurs de qualification juridique et de droit à estimer que ses solutions de circonscription territoriale ne permettent pas d'assurer une protection efficace des droits garantis par le déréférencement.

La position de la CNIL part du constat que, quels que soient les efforts de Google Inc. pour faire coïncider ses terminaisons nationales avec les frontières des Etats, il est en pratique loisible à tout internaute, sans aucune difficulté technique, d'effectuer volontairement sa recherche sur des terminaisons non européennes et d'accéder ainsi, à partir du nom d'une personne, aux résultats déréférencés sur la version nationale. Il est vrai que la redirection automatique ne fonctionne pas quand l'internaute saisit dans sa barre d'adresse une terminaison nationale qui ne correspond pas à sa localisation. Et si elle s'active automatiquement quand l'internaute saisit l'adresse www.google.com, un lien « Utiliser google.com » lui permet de la refuser.

Cette controverse a conduit la société Google Inc. à proposer en cours d'instruction devant la CNIL une solution complémentaire, permettant de fiabiliser le cloisonnement géographique mis en place. C'est la solution dite de « géoblocage », par laquelle la société, en réponse à une demande de déréférencement formulée par une personne déclarant résider en France et en plus du déréférencement sur l'extension nationale, interdit aux internautes localisés physiquement en France grâce à l'adresse IP de leur terminal informatique d'accéder aux résultats concernés. Mais là encore, la CNIL estime trop forts les risques de contournement. Il est ainsi très facile de truquer sa localisation en utilisant un proxy-web, site internet à partir duquel on peut effectuer ses recherches en utilisant non pas sa propre adresse IP, mais celle, fictive, du proxy. Dans le même registre, certains navigateurs dotés d'un VPN[6] intégré proposent à l'internaute de rattacher son adresse IP au pays de son choix. Les internautes les plus dégourdis peuvent installer leur propre VPN, leur permettant de se connecter à internet via une adresse IP localisée par exemple aux Etats-Unis.

Google Inc. a beau souligner que 95% des recherches sont effectuées depuis les terminaisons nationales correspondant aux adresses IP et que la falsification de ces dernières est nécessairement marginale, la CNIL rétorque que les internautes les plus motivés pour débusquer des données personnelles, d'ailleurs incités à le faire par l'avertissement qui paraît sur la page de résultats selon lequel des données personnelles ont pu être déréférencées, peuvent parvenir à leurs fins.

Là encore, ce sont deux visions du droit au déréférencement qui s'opposent : pour Google Inc., le droit au respect des données n'étant pas absolu, sa mise en œuvre par google search peut s'accorder d'une marge d'erreur, d'autant plus réaliste que les données restent de toute façon consultables via d'autres moteurs de recherche ou la saisie d'autres mots clefs. Pour la CNIL, la pesée entre le droit au respect des données, qui n'est certes pas absolu, et les autres impératifs qu'il convient de prendre en compte s'effectue en amont du choix de déréférencer. Une fois le déréférencement acquis, la bulle qu'il instaure doit, indépendamment de son périmètre, être d'une opacité totale.

S'agissant donc à nouveau de déterminer la consistance du droit inventé par la CJUE, nous estimons qu'il n'appartient qu'à elle de se prononcer. Nous le pensons d'autant plus que l'étude de sa jurisprudence rend sa réponse difficilement prévisible. Car si la volonté de donner un effet utile aux règles européennes l'a parfois rendue allante sur l'extraterritorialité (v., s'agissant d'exporter les valeurs de l'Union en matière d'expérimentations animales, CJUE, European Federation for cosmetic ingredients, C-592/14), il lui est aussi arrivé, dans le domaine de la protection des données sur lequel elle se montre pourtant sourcilleuse (CJUE, GC, 8 avril 2014, Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a., C-293/12 et C-594/12 ; CJUE, GC, 21 décembre 2016, Tele2 Sverige AB et Secretary of State for the Home Department, C-698/15 et C-203/15), de refuser des approches englobantes qui auraient des conséquences extraterritoriales disproportionnées (v. CJCE, 6 novembre 2003, Lindqvist, C-101/01, retenant une interprétation stricte de la notion de « transfert vers un pays tiers » pour éviter de faire obstacle à la mise en ligne de données chaque fois qu'un seul Etat tiers n'aurait pas assuré un niveau de protection adéquat ; CJCE, GC, 12 juillet 2011, L'Oreal c. Ebay, C-324/09, limitant l'application de la directive sur la protection des marques aux cas où les sites de vente en

6 Virtual Private Network.

ANNEX 1 : CONCLUSIONS DE MME LA RAPPORTEURE PUBLIC AURÉLIE BRETONNEAU

ligne s'adressent à des consommateurs européens, afin de ne pas soumettre indûment au droit de l'Union des sites destinés à des consommateurs d'Etats tiers au seul motifs qu'ils ont consultables depuis le territoire de l'Union).

Ce choix de renvoyer la question à la CJUE se double de fortes considérations d'opportunité.

S'il est toujours bon que le droit de l'Union européenne fasse l'objet d'une application homogène sur l'ensemble du territoire des Etats membres, il en va a fortiori ainsi quand est en jeu une question de territorialité. Les risques de conflits de normes que porte en germe l'universalité du réseau qui interconnecte des individus appartenant à des systèmes juridiques distincts seraient encore aggravés si, au sein d'un même ordre juridique, les façons d'appliquer le droit différaient.

Or il n'existe parmi les Etats membres de consensus ni sur la portée territoriale du déréférencement, ni sur les mérites comparés de l'approche par nom de domaine ou du géoblocage. Emblématique sont à cet égard les prises de position du G29, qui n'est jamais sorti d'une certaine ambiguïté. Dans sa publication du 26 novembre 2014, il affirme d'abord que le droit au déréférencement ne doit pas être contourné, mais retient quelques lignes plus loin une formulation prudente affirmant qu'il ne doit pas être aisément contourné. Il affirme tout à la fois qu'un déréférencement limité aux extensions européennes ne suffit pas et qu'il doit être appliqué sur l'extension .com, tout en limitant sa portée aux « domaines pertinents », ce qui semble exclure un déréférencement global. Quant aux solutions techniques, il affirme qu'elles pourraient dépendre de l'organisation interne et de la structure des moteurs de recherche. De leurs côtés, une grande majorité d'Etats membres semble, via les prises de position de leurs autorités de régulation, s'être satisfaits d'un déréférencement sur les seules terminaisons européennes, certains (le Royaume-Uni, l'Espagne, voire le Portugal) ayant exigé en complément un géoblocage national. On recense également une décision de la cour régionale de Hambourg se satisfaisant d'un déréférencement limité au territoire de l'Allemagne. La position de la CNIL semble à ce jour assez isolée, le Conseil d'Etat français étant du même coup la première juridiction suprême à être saisie de la question.

Dans le reste du monde enfin, la controverse entre défenseurs et détracteurs du droit au déréférencement est loin d'obéir au partage manichéen entre monde anglo-saxon et Europe continentale auquel on le réduit parfois. On fait ainsi grand cas de l'affaire Equustek (13 juin 2014, Equustek Solutions Inc. v. Jack, BCSC 1063[7]) dans laquelle la Cour suprême de la Colombie-Britannique a, pour pallier les effets d'une concurrence déloyale, exigé de Google qu'il déréférence les liens menant vers le site de l'entreprise contrevenante sur l'ensemble des extensions de google search, seule mesure permettant d'assurer la protection effective des droits de l'entreprise lésée. L'éventail des positions de la doctrine, dont une partie substantielle préconise une voie tierce consistant à ajuster le champ du déréférencement au cas particulier de chaque demande, semble aussi large qu'est vive la controverse à leur sujet. Une position de la CJUE valant pour toute l'Union européenne est particulièrement attendue dans ce contexte.

Au vu de l'ensemble de ces considérations, nous vous proposons de demander à la CJUE si le droit au déréférencement consacré dans son arrêt Google Spain doit être interprété en ce sens que l'exploitant d'un moteur de recherche est tenu, pour y faire droit, de le pratiquer sur l'ensemble des noms de domaine de son moteur, de sorte que les liens litigieux n'apparaissent plus quel que soit le lieu à partir duquel la recherche sur le nom du demandeur est effectuée, ou s'il lui faut seulement veiller à ce qu'il n'apparaissent plus dans les recherches effectuées depuis l'Europe. Au cas où elle opterait pour la seconde branche de l'alternative, nous proposons de lui demander si le déréférencement doit s'effectuer sur l'extension nationale correspondant à l'Etat du demandeur, ou sur l'ensemble des extensions européennes, et s'il doit s'accompagner ou nom d'une mesure dite de géoblocage, dont il faut déterminer le périmètre.

Tel est le sens de nos conclusions.

7 NB : Postérieurement à la séance publique et au prononcé de ces conclusions, la Cour suprême du Canada a confirmé l'injonction de déréférencement global en estimant notamment que « L'Internet n'a pas de frontières (…) Son habitat naturel est mondial. La seule façon de s'assurer que l'injonction atteigne son objectif est qu'elle s'applique là où Google opère – mondialement. »

ANNEX 2 : TABLEAU COMPARATIF DES DIFFÉRENTES VERSIONS DE L'ARTICLE 17 DU RGPD

- ~~Texte barré~~ : partie supprimée
- **Texte en gras : texte modifié**

Proposition de la Commission Européenne adoptée le 25 janv. 2012	**Position du PE adopté le 12 mars 2014**	**Position du Conseil adopté le 15 juin 2015**	**Formulation finale dans le RGPD**
Article 17 Droit à l'oubli numérique et à l'effacement	Article 17 : Droit ~~à l'oubli numérique~~ et à l'effacement	Article 17 : Droit à l'effacement («droit à l'oubli»)	Article 17 : Droit à l'effacement («droit à l'oubli»)
1. La personne concernée a le droit d'obtenir du responsable du traitement l'effacement de données à caractère personnel la concernant et la cessation de la diffusion de ces données, en particulier en ce qui concerne des données à caractère personnel que la personne concernée avait rendues disponibles lorsqu'elle était enfant, ou pour l'un des motifs suivants: a) les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées, b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou lorsque le délai de conservation autorisé a expiré et qu'il n'existe pas d'autre motif légal au traitement des données; c) la personne concernée s'oppose au traitement des données à caractère	1. La personne concernée a le droit d'obtenir du responsable du traitement l'effacement de données à caractère personnel la concernant et la cessation de la diffusion de ces données, ~~en particulier en ce qui concerne des~~ et **d'obtenir de tiers l'effacement de tous les liens vers** ces données à caractère personnel que la personne concernée avait rendues disponibles lorsqu'elle était enfant, **ou de toute copie ou reproduction de celles-ci**, pour l'un des motifs suivants: a) les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées; b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou lorsque le délai de conservation autorisé a expiré et qu'il n'existe pas d'autre motif légal au traitement des données; c) la personne concernée s'oppose au	1. La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, **dans les meilleurs délais**, de données à caractère personnel la concernant et **le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais**, lorsque l'un des motifs suivants s'applique: a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées **d'une autre manière;** b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement; c) la personne concernée s'oppose au traitement en vertu de l'article 21,	1. La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique: a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière; b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement; c) la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée

ANNEX 2 : TABLEAU COMPARATIF DES DIFFÉRENTES VERSIONS DE L'ARTICLE 17 DU RGPD

au traitement des données à caractère personnel en vertu de l'article 19; d) le traitement des données n'est pas conforme au présent règlement pour d'autres motifs. 2. Lorsque le responsable du traitement visé au paragraphe 1 a rendu publiques les données à caractère personnel, il prend toutes les mesures raisonnables, y compris les mesures techniques, en ce qui concerne les données publiées sous sa responsabilité, en vue d'informer les tiers qui traitent lesdites données qu'une personne concernée leur demande d'effacer tous liens vers ces données à caractère personnel, ou toute copie ou reproduction de celles-ci. Lorsque le responsable du traitement a autorisé un tiers à publier des données à caractère personnel, il est réputé responsable de cette publication.	traitement des données à caractère personnel en vertu de l'article 19; c bis) **une juridiction ou une autorité réglementaire basée dans l'Union a jugé que les données concernées doivent être effacées et cette décision est passée en force de chose jugée;** d) ~~le traitement des~~ les données ~~n'est pas conforme au présent règlement pour d'autres motifs.~~ ont fait l'objet d'un traitement illicite . 1 bis. **L'application du paragraphe 1 dépend de la capacité du responsable du traitement à vérifier que la personne demandant l'effacement est la personne concernée.** 2. Lorsque le responsable du traitement visé au paragraphe 1 a rendu publiques les données à caractère personnel **sans aucune justification fondée sur l'article 6, paragraphe 1,** il prend toutes les mesures raisonnables **pour que ces données soient effacées,** y compris ~~les mesures techniques, en ce qui concerne les données publiées sous sa responsabilité, en vue d'informer les tiers qui traitent lesdites données qu'une personne concernée leur demande d'effacer tous liens vers ces données à caractère personnel, ou toute copie ou reproduction de celles-ci. Lorsque le~~ **par des tiers, sans préjudice de l'article 77**. Le responsable du	paragraphe 1, et **il n'existe pas de motif légitime impérieux pour le traitement,** ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2; d) les données à caractère personnel ont fait l'objet d'un traitement illicite; e) **les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis;** f) **les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1.** 2. Lorsqu'il a rendu publiques les données à caractère personnel et qu'il est tenu de les effacer en vertu du paragraphe 1, le responsable du traitement, compte tenu des **technologies disponibles** et des **coûts de mise en œuvre**, prend des mesures raisonnables, y compris **d'ordre technique,** pour informer les responsables du traitement qui traitent ces données à caractère personnel que la personne concernée a demandé	s'oppose au traitement en vertu de l'article 21, paragraphe 2; d) les données à caractère personnel ont fait l'objet d'un traitement illicite; e) les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis; f) les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1. 2. Lorsqu'il a rendu publiques les données à caractère personnel et qu'il est tenu de les effacer en vertu du paragraphe 1, le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre technique, pour informer les responsables du traitement qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci.

ANNEX 2 : TABLEAU COMPARATIF DES DIFFÉRENTES VERSIONS DE L'ARTICLE 17 DU RGPD

3. Le responsable du traitement procède à l'effacement sans délai, sauf lorsque la conservation des données à caractère personnel est nécessaire: a) à l'exercice du droit à la liberté d'expression, conformément à l'article 80; b) pour des motifs d'intérêt général dans le domaine de la santé publique, conformément à l'article 81; c) à des fins de recherche historique, statistique et scientifique, conformément à l'article 83; d) au respect d'une obligation légale de conserver les données à caractère personnel prévue par le droit de l'Union ou par la législation d'un État membre à laquelle le responsable du traitement est soumis; la législation de l'État membre doit répondre à un objectif d'intérêt général, respecter le contenu essentiel du droit à la protection des données à caractère personnel et être proportionnée à l'objectif légitime poursuivi; e) dans les cas mentionnés au paragraphe 4.	traitement ~~a autorisé un~~ **informe la personne concernée, lorsque cela est** possible, des mesures prises par les tiers ~~à publier des données à caractère personnel, il est réputé responsable de cette publication.~~ **concernés.** 3. Le responsable du traitement ~~procède~~ **et, le cas échant, le tiers procèdent** à l'effacement sans délai, sauf lorsque la conservation des données à caractère personnel est nécessaire: a) à l'exercice du droit à la liberté d'expression, conformément à l'article 80; b) pour des motifs d'intérêt général dans le domaine de la santé publique, conformément à l'article 81; c) à des fins de recherche historique, statistique et scientifique, conformément à l'article 83; d) au respect d'une obligation légale de conserver les données à caractère personnel prévue par le droit de l'Union ou par le droit d'un État membre auquel le responsable du traitement est soumis; le droit de l'État membre doit répondre à un objectif d'intérêt général, respecter l'essence du droit à la protection des données à caractère personnel et être proportionné à l'objectif légitime poursuivi;	l'effacement par ces responsables du traitement de **tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction** de celles-ci. 3. Les paragraphes 1 et 2 ne s'appliquent pas dans la mesure où ce traitement est nécessaire: a) à l'exercice du droit à la liberté d'expression et d'information; b) pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement; c)pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, paragraphe 2, points h) et i), ainsi qu'à l'article 9, paragraphe 3; d) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre	3. Les paragraphes 1 et 2 ne s'appliquent pas dans la mesure où ce traitement est nécessaire: a) à l'exercice du droit à la liberté d'expression et d'information; b) pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement; c) pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, paragraphe 2, points h) et i), ainsi qu'à l'article 9, paragraphe 3; d) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement; ou e) à la constatation, à l'exercice ou à la défense de droits en justice.

ANNEX 2 : TABLEAU COMPARATIF DES DIFFÉRENTES VERSIONS DE L'ARTICLE 17 DU RGPD

4. Au lieu de procéder à l'effacement, le responsable du traitement limite le traitement de données à caractère personnel: a) pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données lorsque cette dernière est contestée par la personne concernée; b) lorsqu'elles ne sont plus utiles au responsable du traitement pour qu'il s'acquitte de sa mission, mais qu'elles doivent être conservées à des fins probatoires, ou c) lorsque leur traitement est illicite et que la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation; d) lorsque la personne concernée demande le transfert des données à caractère personnel à un autre système de traitement automatisé, conformément à l'article 18, paragraphe 2.	e) dans les cas mentionnés au paragraphe 4. 4. Au lieu de procéder à l'effacement, le responsable du traitement limite le traitement de données à caractère personnel **de manière à ce qu'elles ne soient pas soumises aux manipulations usuelles d'accès aux données et de traitement des données et qu'elles ne puissent plus être modifiées :** a) pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données lorsque cette dernière est contestée par la personne concernée; b) lorsqu'elles ne sont plus utiles au responsable du traitement pour qu'il s'acquitte de sa mission, mais qu'elles doivent être conservées à des fins probatoires ; ou c) lorsque leur traitement est illicite et que la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation; c bis) **lorsqu'une juridiction ou une autorité réglementaire basée dans l'Union a jugé que le traitement des données concernées doit être limité et cette décision est passée en force de chose jugée;**	gravement la réalisation des objectifs dudit traitement; ou e) à la constatation, à l'exercice ou à la défense de droits en justice.	

ANNEX 2 : TABLEAU COMPARATIF DES DIFFÉRENTES VERSIONS DE L'ARTICLE 17 DU RGPD

5. Les données à caractère personnel énumérées au paragraphe 4 ne peuvent être traitées, à l'exception de la conservation, qu'à des fins probatoires, ou avec le consentement de la personne concernée, ou aux fins de la protection des droits d'une autre personne physique ou morale ou pour un objectif d'intérêt général. 6. Lorsque le traitement des données à caractère personnel est limité conformément au paragraphe 4, le responsable du traitement informe la personne concernée avant de lever la limitation frappant le traitement. 7. Le responsable du traitement met en œuvre des mécanismes assurant le respect des délais applicables à l'effacement des données à caractère personnel et/ou à un examen périodique de la nécessité de conserver ces données. 8. Lorsque l'effacement est effectué, le responsable du traitement ne procède à aucun autre traitement de ces données à caractère personnel. 9. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser:	d) lorsque la personne concernée demande le transfert des données à caractère personnel à un autre système de traitement automatisé, conformément à l'article 18 15 , paragraphe 2 2 bis. d bis) **lorsque le type particulier de technologie de stockage ne permet pas l'effacement et a été mis en place avant l'entrée en vigueur du présent règlement.** 5. Les données à caractère personnel visées au paragraphe 4 ne peuvent être traitées, à l'exception de la conservation, qu'à des fins probatoires, ou avec le consentement de la personne concernée, ou aux fins de la protection des droits d'une autre personne physique ou morale ou pour un objectif d'intérêt général. 6. Lorsque le traitement des données à caractère personnel est limité conformément au paragraphe 4, le responsable du traitement informe la personne concernée avant de lever la limitation frappant le traitement. 7. ~~Le responsable du traitement met en œuvre des mécanismes assurant le respect des délais applicables à l'effacement des données à caractère personnel et/ou à un examen périodique de la nécessité de conserver ces données.~~		

ANNEX 2 : TABLEAU COMPARATIF DES DIFFÉRENTES VERSIONS DE L'ARTICLE 17 DU RGPD

a) les exigences et critères relatifs à l'application du paragraphe 1 dans des secteurs spécifiques et des situations spécifiques impliquant le traitement de données; b) les conditions de la suppression des liens vers ces données à caractère personnel, des copies ou des reproductions de celles-ci existant dans les services de communication accessibles au public, ainsi que le prévoit le paragraphe 2; c) les conditions et critères applicables à la limitation du traitement des données à caractère personnel, visés au paragraphe 4.	8. Lorsque l'effacement est effectué, le responsable du traitement ne procède à aucun autre traitement de ces données à caractère personnel. 8 bis. **Le responsable du traitement met en œuvre des mécanismes assurant le respect des délais applicables à l'effacement des données à caractère personnel et/ou à un examen périodique de la nécessité de conserver ces données.** 9. La Commission est habilitée à adopter, **après avoir demandé l'avis du comité européen de la protection des données,** des actes délégués en conformité avec l'article 86, aux fins de préciser: a) les exigences et critères relatifs à l'application du paragraphe 1 dans des secteurs spécifiques et des situations spécifiques impliquant le traitement de données; b) les conditions de la suppression des liens vers ces données à caractère personnel, des copies ou des reproductions de celles-ci existant dans les services de communication accessibles au public, ainsi que le prévoit le paragraphe 2; c) les conditions et critères applicables à la limitation du traitement des données à caractère personnel, visés au paragraphe 4. [Am. 112]		