The Right to Data Protection: European Exceptionalism or a Fundamental Right?

Dr. Vasiliki Christou[*]

A. Introductory Remarks

In most European countries data protection is guaranteed as part of a fundamental right to privacy. This coming May the entry into force of the new European Regulation on data protection, namely of the GDPR (General Data Protection Regulation), has already caused a general alert to businesses aiming to timely adjust to the new requirements to avoid very high fines. On the other hand, American businesses have been registering under the Privacy Shield after the Safe Harbor Agreement was struck down by the European Union Court (Schrems case)[1] as failing to satisfy an adequate level of protection with respect to data being transferred to the USA. The Privacy Shield Agreement is currently under review by the European Union Court and nobody knows what comes out.[2]

Why do Europeans do that? Why do they insist so much on a data protection right? Is it more efficient for the European economy? Is it a European peculiarity, European exceptionalism or even a European indulgence in being the human rights protection leader in the Globe? Is there a data protection right or have the Europeans gone too far? What is there to protect about information that is not fake or false and that does not concern private life in a free and democratic society?

My view, which I have elaborated in my book on the Right to Data Protection published in Greek beginning of past year,[3] is that a right to data protection touches upon fundamental aspects of autonomy. However, it functions most of the times not as categorically or in absolute terms forbidding an action, as the case may be with

---

[*] Adjunct Professor at the European Law and Governance School, Attorney at Law, Athens, Greece.
The present paper is Work in Progress. Please do not cite.

[1] C-362/2014, M. Schrems v. Ireland, November 6, 2015.

[2] See 17N/ WP 255, EU-US Privacy Shield. First Annual Joint Review, November 28, 2017

[3] Vasiliki Christou, Το δικαίωμα στην προστασία από την επεξεργασία δεδομένων. Θεμελίωση – Ερμηνεία – Προοπτικές, πρόλογος Νίκος Κ. Αλιβιζάτος (The Right to Data Protection. Foundation – Interpretation – Prospects, introduction by Nikos K. Alivizatos), Athens – Thessaloniki, Sakkoulas Publications, 2017.

freedom of speech,[4] or as a strong right in the meaning of Dworkin,[5] but rather as setting a process and some safeguards about the flow of information in the so-called back in the 1970s[6] Dossier Society and now in the Internet Society. Not including, in my view, a categorical imperative, an absolute, the right to data protection may be balanced against competing interests or rights and may be outweighed or restricted by them. The much beloved in European human rights jurisprudence principle of proportionality plays indeed an important role in accommodating the right to data protection as well as the individual (the data subject) in a democracy and in a society. To my mind, opposite to other human rights, such as freedom of conscience and belief, the right to data protection is not constitutive of the abstract self[7] before her entrance to a Social Contract, it is not itself a precondition for entering the Social Contract within the meaning of Rawls, that is the Original Position or the reflective equilibrium, but it is constitutive of an embedded identity in the liberal and democratic society.

In the following I shall present first (under B), what the foundations of the right to data protection are, to my mind, and second (under C), how such right may be reconciled with freedom of expression. Before that however I would like to clarify that the right to data protection should not be understood as similar or related to the notion of privacy in the common law. If we take a look at the four torts related to privacy protection in common law, namely a) intrusion of one's solitude by the publication of private facts, b) placing somebody under false light, c) appropriation of one's name without consent and d) infliction of emotional distress[8], then none of these aspects of privacy protection has anything to do with the right to data protection, as I am interpreting it here from the perspective of European legislation. Invasion to private life or property (if my name is my property), defamation or distress

[4] See for example Ronald Dworkin, Rights as Trumps, in Waldron (ed.), Theories of Rights, Oxford: Oxford University Press, 153, and Alan Gewirth, Are There Any Absolute Rights?, in Waldron (ed.), Theories of Rights, 91.

[5] Ronald Dworkin, Taking Rights Seriously, London: Duckworth 1971, 191-200.

[6] Arthur Miller, The Assault on Privacy. Computers, Data Banks and Dossiers, 1970. See also Stanton Wheeler (ed.), On Record: Files and Dossiers in American Life, New York: Russell Sage, 1969.

[7] Compare Christine Korsgaard, Self-Constitution: Agency, Identity and Integrity, Oxford: Oxford University Press, 2009.

[8] William L. Prosser, Privacy, 48 California Law Review 383 (1960).

are not circumstances to be dealt with by the right to data protection. Then what is the right to data protection all about?

B. Foundations of the Right to Data Protection

1. Negative Liberty Perspective: Behavioral Privacy

a. Freedom from Being Monitored, Tracked or Recorded

First, I have to explain the meaning of privacy as will be used here, because differences in the meaning ascribed to privacy in various legal orders, as already indicated, have cared for crucial misunderstandings and confusion about the content of privacy and data protection. I differentiate between privacy and private life. The right to private life refers to the protection of fundamental aspects of an individual's intimate sphere, sex and love life, and health. Such right must indeed be very strictly, categorically (that is almost unexceptionally) protected, but has little to do with the right to data protection. Information about private life in the above sense has been traditionally protected, and we needed not invent a new right (at some time in the 1970s) to address such issue. The idea of a right to data protection poses a question that comes next and lies beyond the long-established protection of private data. To put it in a nutshell, the right to data protection primarily raises the question of how we deal with information about our social life, and this is why I mentioned in the introductory remarks that the data protection right is about the constitution, not of the self, but of a liberal and democratic society itself.

So, when I speak of privacy as a foundation of the right to data protection, I certainly do not mean private life. I speak of privacy as a general condition of autonomy, expressing the main idea of respect to the choices of an individual. Respect in that sense is demonstrated by lack of interference with other people's choices. Behavioral privacy, as a special aspect of privacy, is freedom to behave in the public sphere without being followed, attended or observed, freedom to experiment with new ways and attitudes of life, and with new ideas.[9] Freedom from observation is significant, because it equates to freedom from censorship or self-censorship, and it disentangles

[9] See for example Alan Westin, Privacy and Freedom, New York: Atheneum, 1967, 33: "[T]here are aspects of [oneself] that the individual does not fully understand but is slowly exploring and shaping as he develops".

the individual from the restraints of a feeling of an obligation to obey: when under watch, the individual tends to show that she obeys to the rules of the one watching her, the other being clearly in a dominant position. In such circumstances the individual also tends to adjust her behavior to the desires of the one watching her, so that she is approved and popular. The way to implement freedom from observation and attendance is to be free from monitoring, tracking, or recording. Behavioral privacy is an "unrecorded" privacy that aims at freedom to unfold one's personality in the social and public sphere, to act spontaneously and without precaution. In that way behavioral privacy is favoring free expression.[10] No speech can be freer than the oral, unrecorded one. The capability to act unpretentiously is of fundamental importance for human development.

The demand for behavioral privacy has become quite pressing nowadays. CCTV in public and semi-public social sphere, "cookies" everywhere in the cyber-environment, widespread GPS, and all kinds of interconnections between digital services providers have decreased quite significantly the opportunities an individual has to remain unattended in the public sphere. If you add to it the fact that in the "clouds" there is no space storage limitation, then not only is one systematically tracked and attended but her tracks may never be erased, had there not been a right to data protection to set some procedural rules.

Taking the systematic monitoring of modern individuals under consideration, it is not an exaggeration to say that the naked resident of the Samoa Islands described in the book of Margaret Mead,[11] enjoyed much more privacy than we do today. It was the privacy of the moment that went unrecorded and became precious because of its uniqueness in a lifetime. That moment would not be replayed in the future in unknown and irrelevant contexts and nobody would have to account for it. It was also the privacy of the particular audience, of the particular group of people that had come together either by choice or by chance but - what is important – in real life, in the field, exposed to personal interaction, heat and temperature, either physical or

[10] Timothy Garton Ash, Free Speech. Ten Principles for a Connected World, London: Atlantic Books, 2016, 285: "the ability to choose what you wish to keep private, and then to have confidence that this choice will be respected, is […] a condition [of free speech]".
[11] Margaret Mead, Coming of Age in Samoa, New York, 1949, 82-85.

psychical. In that sense I believe that privacy of the body may be a culture specific good but behavioral privacy is a universal value. That explains why Germans are strongly opposed to the establishment of CCTV in the public space, but they are much less annoyed by people sunbathing naked in public parks or on the river banks.[12]

b. Freedom from Profiling

There are various mechanisms to further process the information collected by monitoring, tracking and recording, which may be summarized under the term "data mining" with the purpose of "profiling". Profiling is a technique of mass data surveillance of groups of people, and search of the data to match individuals to a profile. Search engines identify patterns of behavior of Internet users (or the users of the informational system of a corporation), which are then primarily used for crime prevention and detection, for commercial purposes with high financial returns (behavioral advertising) or to evaluate persons (i.e. employees) or even prognose diseases (of potential clients of insurance companies). Unrestricted submission of an individual's information to a research process by public or private entities transforms the data subject into an object or, in other words, renders the individual a means to serve some other end. From a constitutional law perspective, the problem with profiling is twofold: on the one hand, to use suspect criteria, such as race, gender or religious beliefs, at the process of profiling infringes Equality Clause or the principle of non-discrimination. On the other hand excessive profiling, not narrowly tailored to the achievement of specific goals, which may not be pursued otherwise, has the tendency to dehumanize the decision making process and reduce an individual down to her information. Respect for human dignity means from a Kantian perspective not to instrumentalize humans to achieve goals not determined by them (crime prevention or economic profit). It also means to recognize the other as a person, and not as an aggregate of information. We are not just our information, we are the way we look, we laugh and stand, the way we respond to humor, the way we show awkwardness in the face of surprise or threat. Under the light of a right to data protection, law seams to acknowledge that to know a person (and thus to be able to make a significant decision about her with fairness) is to have some experience of her,

[12] See Ash, Free Speech, 287.

and not just of her information, combined under some algorithm. Besides, much prejudice may be hidden behind tons of facts.

In this direction, GDPR includes a right to obtain human intervention in case of automated decision making including profiling. According to Recital 71 "[t]he data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention". The GDPR also defines profiling as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements", and prohibits solely automated decision making including profiling, if the decision produces legal effects concerning the data subject or similarly significantly affects him or her (Art. 22 GDPR). This means that prior to every significant decision affecting the individual, a meaningful oversight of the decision by a human has to take place. According to WP 29 an oversight may be meaningful only, if carried out by someone who has the appropriate authority and competence to change the decision. Also an analysis of all input and output data has to take place.[13] If an individual has exceptionally been submitted to solely automated decision making for some overriding public interest, such as fighting against fraud, money laundering or tax evasion, then the data subject has the right to request and obtain human intervention by challenging the decision taken. In such case the data subject is entitled to a meaningful review of the decision in the above sense, whereas not only input and output data, but also additional elements, not already considered, need to be reviewed.[14] Last the GDPR sets some strict transparency rules about profiling. Again the right to data protection sets some procedural constraints to the processing of information, rather than an absolute prohibition. Therefore a controller

[13] 17/EN WP 251, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, October 3, 2017, p. 10.
[14] O.c, p. 15.

implementing profiling should take all appropriate measures to inform the data subject, in a simple and easily understandable way (that is not by demonstrating some algorithm) about the logic and the consequences of processing, how a profile is built and how it is relevant to the decision, about the data collected, but also about the data derived: the information produced by the processing itself.[15] Furthermore the data subject may object not only to the processing, but may also challenge the reliability of criteria used to produce a behavior pattern, the way the criteria are combined and the outcome data themselves.

2. Positive Liberty Perspective: Informational Privacy

a. Freedom to Participate in the Social and Public Sphere

In this second part I shall try to introduce another foundation and justification of the right to data protection, called informational privacy in some common law readings or "informational self-determination" (informationelle Selbstbestimmung) in Germany. Informational privacy is positive in nature. It secures freedom to do something rather than freedom from interference. In 1967, Alan Westin in his famous book on privacy summarized under "informational privacy" the claims of the individual to determine when, how and to what extent information relating to it would be disclosed or notified to others.[16] In 1984 the Constitutional Court of Germany in its famous "Volkszählunsurteil" declared the right to informational self-determination as the right of the individual to have overview and some control over the flow of data concerning her. Under that perspective the Constitutional Court declared the law that specified the categories of data to be collected at the census as invalid, because the data collected were not narrowly tailored to serve the purpose of a census, on the contrary several irrelevant data were also collected. At the social background of the decision of the Court, there was great concern and agitation about the dangers of the upcoming computer age for the human personality and development. In the public

[15] O.c., p. 28.
[16] Westin, Privacy and Freedom, 1967, 7.

debate of the time the risks of computers' usage for the individual were compared to the risks of nuclear energy for environmental pollution.[17]

In its decision, the Constitutional Court was concerned with the fact that the individual's freedom of decision is interfered with, if the flow of information concerning her is not transparent and to some extent dependent upon her consent. Following phrase of the Court has traditionally been cited as the gist of the argument: *Anyone who cannot be sure with sufficient certainty what information about her has been made known to certain areas of social life and who is not aware who the individuals are, with which she should establish some communication, because they already know information about her - if anything to update and control the accuracy of such information - she is prevented from exercising her freedom to plan her life and decide at her own will.*[18] In other words the Court aimed at guaranteeing an informed decision-making process for the individual and an effective participation capability in public and social life. Spyros Simitis, Founder of the first, worldwide, data protection law in the Land of Hesse and subsequently of the German Federal Law payed also great attention, in his relevant writings, to the value of fair participation in public and social life under the new circumstances brought about by computer and internet. Simitis summarizes under the notion of "Kontextverlust"[19] (loss of context) the reason why the "new" right was necessary. De-contextualization posed new dangers to individual development. In the cyber environment, information, images and moments circulate freely in the digital clouds above and beyond national boundaries, detached from context, their historical and human surroundings forever. The right to data protection seeks to regulate precisely this, that the pieces of ourselves which by

[17] See Collin Bennett, Regulating Privacy. Data Protection and Public Policy in Europe and the United States, Ithaca and London: Cornell University Press, 1992, 75.

[18] BVerfG 65, 1 (43): Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß".

[19] Spyros Simitis, Einleitung: Geschichte-Ziele-Prinzipien, in Simitis (ed.), Bundesdatenschutzgesetz Kommentar, Baden Baden: Nomos, 2011, 78-79.

modern means are cut off from it, will remain embedded in the sphere of our personality.

The new right aimed at protecting some procedural aspects of an autonomous decision making process and of fair participation. It did not introduce a new material good or value to be protected. It was all about protecting freedom of choice and decision from new dangers, the dangers of de-contextualization of data. In this respect, some scholars, among them predominantly Professor Hans Peter Bull, being the first German Ombudsman for Personal Data, have been skeptical about calling data protection as a new "right", since it added no new content to the fundamental rights catalogue' on the contrary relevant law set "merely" some safeguards of the conditions for the exercise of all freedoms.[20] However, merely procedural rights are nothing new, starting from Procedural Due Process Law to the right to be heard in a court, and, as far as data protection is concerned, preventive protection by setting up a process is of paramount importance, because after a data breach it is difficult to compensate or even calculate or prove the damage done. The fact that the right to data protection aims primarily at preventing dangers, not facing clear and present dangers, also explains why I have considered it as a right that may be open to balancing. The right to data protection offers reasons and arguments about how information society should be organized. It does not dictate absolutes.

b. Freedom to Introduce Myself and to Choose and Fragment My Audience

A second dimension of informational privacy as a form of positive liberty is again primarily of German origin. It is the right to present myself, "Recht auf Selbstdarstellung", perceived as an expansion of the right to one's image, traditionally coming into consideration in case of publication of photos of public figures. I propose rephrasing this right as a right to introduce myself to new audiences, and add to that a right to choose and fragment my audiences, and I shall try to explain what I mean by that. However I would like to make clear from the beginning that a right to present and introduce myself is about enjoying a real chance to tell my story and present my own perception of myself in new surroundings. It does not also constitute a right to

[20] Hans Peter Bull, Informationelle Selbstbestimmung. Vision oder Illusion? Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit, Tübingen: Mohr Siebeck, 2011, 45.

be perceived and judged by others in a particular, desired way. It is about securing a real opportunity to expose what I believe about myself, a real chance to make a new start despite past mistakes. Making a new start and telling one's own story (before I get a new job or move to a new neighborhood), has become more difficult due to the easy resort of anyone to the non-erasable, huge internet memory and the recalling[21] and interconnecting abilities offered. This is why I would like to shed new light on the "German" right to present myself as a right to introduce myself in new settings. I would like to stress the importance of choosing and starting a new life as free as possible from prejudice. Back in the 1960's, at least in Greece, people would move from the villages to the cities to make such a new start and erase their path traces behind. How could we secure such a real chance for a new life in the modern, digital, recorded age?

From a legal point of view the so-called "right to forget or to be forgotten" aims to serve such purpose. Such right has always been foreseen in European data protection law as a "right to erasure". However, the famous Google Spain decision of the European Court of Justice in 2014[22] made it more explicit and, following that, the GDPR included a special Article on the right to be forgotten (Article 17 GDPR). The European Court of Justice ruled that Google is obliged, after a relevant request by the data subject, not to allow, but to "block" the retrieval of certain websites, when the search is made by name and surname, and the information presented on these websites is of no public interest. The Court remarkably and to my mind successfully enough stroke a balance between the right to be forgotten and free speech, by declaring that the former may not be raised against electronic newspapers containing the same information, but only on search engines. To my mind, the Court understood where the heart of the problem was: the problem was not the dissemination of information, even by electronic means; the problem was the new interconnection abilities that would allow easily placing someone on the spot anytime.

[21] See J.-Fr. Blanchette, The Noise in the Archive: Oblivion in the Age of Total Recall, in: Gutwirth/Poullet/De Hert/Leenes (eds.), Computers, Privacy and Data Protection: an Element of Choice, Dordrecht/Heidelberg/London/New York: Springer, 2011, 25.
[22] C-131/12, Google Spain, May 13, 2014.

Article 17 GDPR includes a quite detailed formulation of the right to be forgotten that engages multiple criteria and a lot of balancing that has thus already caused a lot of frustration in the legal departments of the industry about how it should be implemented. Frustration has also been caused because, even after the decision for deletion has been reached, implementation of deleting is not easy. Not only because the most effective way to delete information in digital environment is secure cryptography, but also because it may not be easy to locate where personal data has been stored. One very common example of this occurs, when, due to remote connection one may access email or other information from a number of local devices, possibly not under the control of the Data Controller himself.

In any case, Article 17 guarantees the right of the data subject to have personal data concerning her erased, where the retention of such data is no longer necessary in relation to the purposes for which they are collected or otherwise processed. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defense of legal claims. It is clear from the above that the GDPR offers very little help with regards to balancing between right to be forgotten and freedom of expression, which to my mind shall be carried out based on traditional criteria, such as the public official/public figure classification or the public interest relevance of the crucial data.

Much as the right to be forgotten has been contested, it is not however utterly new. As already mentioned, a right to erasure has always been foreseen in European legislation. Additionally a right to oblivion had, quite early, in the year 1973, been discussed by the constitutional court of Germany in the so called Lebach decision.[23] In the Lebach case ZDF, one of the two biggest public TV Stations in Germany, had displayed a documentary about the criminal deeds of the applicant, emphasizing the

[23] BVerfG 35, 202 (233).

applicant's homosexuality, at exactly the time he was released from prison. The Federal Constitutional Court ruled that the documentary, presented on the TV at the particular time interfered with the applicant's real resocialization chances. The Constitutional Court declared that individual claims for fair participation in society may pose restrictions to the right of the public to be informed about a criminal's past deeds and his private life. Moreover the European Court of Human Rights in the year 2006 ruled that archives concerning political opponents of the Gold War era formed by the secret services may not be retained eternally and should have been by the time destroyed.[24] Last, Stone and Warner, already in 1969 pointed out that "[t]he computer has given the bureaucracy the gift of omniscience, if not of omnipotence, by putting into its hands the power to *know*. No fact unrecorded, nothing forgotten and lost, nothing forgiven"[25].

Forgetting is important to human society. Szekely points out that "[i]n the course of human history, forgetting was the norm and remembering the exception. Now it seems to be the other way around: it is the act of forgetting, or the ability to forget, that is becoming the exception".[26] Remembering is all about selecting what to forget after evaluation and judgement. Information passing that test is valuable, and "their ability to survive is precisely that makes them so precious, lending them a value that they would never have in a world where everything was kept forever".[27] In other words remembering all information forever is, paradoxically enough, a way to devalue them, to make them frivolous. Additionally, revealing and recalling all facts, with no critical selection, is again, paradoxically enough, a way to hide some truth. For there is no better way to hide a secret than under mass detailed information about everything. Forgetting is not only evaluating, judging and laying emphasis on what is selected, it is also forgiving, which is important for social cohesion, tolerance and integration. As Szekely puts it, "[t]he possibility of storing information on everyone, of retrieving and using it at any time against anybody, is the perfect means to detect and

[24] Segerstedt-Wiberg et al v. Sweden, appl. No 62332/00, June 6, 2006, par. 88-92.
[25] M.G. Stone/Malcolm Warner, Politics, Privacy and Computers, The Political Quarterly 1969, 256, 260.
[26] Ivan Szekely, Personal Reflections on the Fate of Personal Data in the Information Society, in Gutwirth/Leenes/De Hert/Poullet (eds.), European Data Protection: In Good Health?, Springer, Dordrecht/Heidelberg/London/New York, 2012, pp. 347 – 363, 347-348.
[27] Szekely, o.c., 349.

sanction the slightest deviation from the ideologically, politically or commercially preferred behavior".[28]

"Total memory" has also affected human development. The individual has – to some degree – lost the capability, even by well-meaning distortions, to reconstruct her past, to make it match the desired perception of herself. What constitutes a person is the choices she makes, and what constitutes the identity of a person are those choices she would gladfully recognize as a coherent reflection of herself.[29]

Besides the right to introduce myself (after forgetting, forgiving, and erasing), there is also another fundamental interest underlying the right to data protection, which I have named more specifically as the right to choose and fragment my audience. I believe that one of the negative consequences of the internet society is that it has brought about the unification of society in terms of both space and time, and under this perspective a "total" society has been created, which is very oppressive to individual freedom. Internet has diminished time, space and storage limitations in a way that it has effectuated what I call, with some exaggeration for the sake of the argument, as "social totalitarianism", in the sense that Internet society, if not regulated properly by such a right as the right to data protection, it will be a total one, one without boundaries between past and present, work and pleasure, friends and relatives. Social Media would be able, if not scrutinized by a right to data protection (underpinning techniques such as privacy by default or privacy by design), to eliminate the possibility of addressing different audiences in different spheres and aspect of our life, in other words the "fragmentation" of the social space.

I shall try to explain how the capability to choose an audience, which is only a segment of the society, to fragment society to different audiences is a very essential part of individual freedom. The privacy of the audience is the underlying idea of the confidentiality of communication, which has a long-established tradition in constitutional jurisprudence. Even where, like in the USA, an all-encompassing right to data protection has not been recognized on a constitutional level, freedom of

[28] Szekely, o.c., 353.

[29] Compare Ash, Free Speech, 305: "[W]e also re-remember our own pasts in ways that make the, more comfortable for our present selves. […] The indelible memory of the Internet threatens both the forgetting that enable us to function and this constant reconstruction of the self".

communication, which equates to private, confidential communication, is considered as a constitutional value. What I wish to show is that the same reason that has led us recognize that free communication is a private one, should make us acknowledge that privacy by design and by default techniques to allow me determine who views what until when, to determine and overview which my audience is, in the social network services are important to human freedom.

In other words, in my view there is a human need to address different audiences in different ways, to play different roles in different settings and to cultivate this complexity as an element of an autonomous being. Timothy Garton Ash has manifested that wonderfully in his recent book on free speech, and I think a strong point is made already by the fact that a book about free speech is also, largely, a book about privacy. He writes: "We all speak differently to different audiences more freely to some, less to others. […] The poet W.H. Aude once observed that if men knew what women said to each other about them, the human race would die out. […] The varies tones and registers we use in different contexts, those infinite shades of irony, parody, understatement and overstatement, of the half spoken and the delicately implied, are the stuff of novels and poetry"[30]. I would add, as the audience widens, delicate implications fade out.

C. Reconciling Data Protection with Free Speech

I have already mentioned that I do not consider the right to data protection as a strong right like freedom of speech, containing some absolutes, on the other hand it is rather a relevant right subject to balancing. It is a right about how to share personal information with others and may not be interpreted as a right of non-diclosure.[31] In this respect I believe that the right to data protection is not applicable in case of publishing, even electronic publishing. Against publications one may use the traditional limitations of free speech. The right to data protection is, to my mind, only about processing of information, dissemination of it not being included, and about being able to overlook further data derived about the person from the initial, the

[30] Ash, Free Speech, 285-286.

[31] Contrary to my view Stavros Tsakyrakis argues in his paper "Is There a General Right of Non-Disclosure?" against the recognition of a data protection right, www.constitutionalism.gr

input data. Such thought underlies, to my mind, the judgement of the European Union Court on Google Spain case, as that judgement did not turn against the publisher, but only against the search engine, as already explained.

However, such view is not uncontested in Europe. First neither Directive 95/46/EC nor the GDPR excluded dissemination of information from the very definition of processing. That would be to solve the tension between freedom of speech and data privacy a priori, by drawing a line with a sharp categorical knife. The reason why this did not happen is to my mind that European human rights jurisprudence is very unfamiliar with defining one right against the other as a way of solving a conflict. European legislators and judges generally feel more comfortable to decide ad hoc in the light of the circumstances than to sort things out on an abstract level. However, Article 9 of the Directive 94/46 did mention that Member States shall provide for exemptions or derogations from most of the provisions of the Directive for processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression. In other words, national legislators were free to free speech of the data privacy restraints, with the exception of the provisions on the security of the data collected. The implementation of this derogation has not been common in the member states. I believe we can differentiate between England, France and Italy favoring problem solving on the basis of ad hoc decisions, thus favoring balancing, and central Europe, such as Germany, Austria, Belgium etc, where it is clear in the law that federal data protection legislation does not apply to the media, including TV and Radio, except for the security of the files. Greece could be considered a category of its own, together perhaps with Cyprus, as in both cases national legislation foresees that a journalist may process and disseminate personal data concerning the private life or health of someone upon authorization by the Data Protection Authority, which would review whether the matter was of public interest. In practice such law provision became, at least in Greece, obsolete, and was practically never applied under the pressure of the constitutional provisions on free speech, banning all sorts of censorship and prior restraint.

The GDPR does not materially differentiate from the Directive although it broadens the derogation to also include university research. Article 85 of the GDPR foresees that Member States shall by law reconcile the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression. Accordingly for processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organizations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

However, I do believe that to exempt the press and the media from the right to data protection is consistent to the justification of such a right, as has been presented in this paper. The justification has not been, I hope, merely theoretical, but it has to a great extent been based upon the real, historic circumstances, under which the right to data protection emerged in Europe. Such circumstances have never been related, as I have tried to show, to the eventual harm of speech, but only to the dangers of automated archiving and then of the Internet.

D. *Conclusion*

The right to data protection has paved its way through the human rights jurisprudence and legislation in Europe very effectively, although the theoretical foundations of such a right have not yet been crystallized. Before entering the new (?) era of the GDPR it is useful to step back and reflect on the basics, gaining from the rich implementation experience of the past decades.