للكاتب: د. منى الاشقر جبور - د. محمود جبور

The right to be forgotten

Mona Al achkarJabbour
Professor of Law
Faculty of Law & Political Sciences- Lebanese University
Maj_aj@hotmail.com

Mahmoud Jabbour
Professor of Political Sciences
Faculty of Law & Political Sciences- Lebanese University
Hannibal.m@hotmail.com

Abstract: Nowadays, we live in the Big Data Era, in an information ecosystem, where many of our actions, researches, photos, and comments, are collected, analyzed and used to predict our behavior, as well as, our likings and inclinations. On the Internet, a simple search will likely lead, to an extensive set of links containing data about any person, which may be untrue, or simply outdated. The scary thing is that this is not designed to be forgotten. With the actual information technologies and communications' capacity, collected personal data and information can be stored and accessed ad infinitum. Hence, Different interests are at stake when information is made public, collected and exchanged on information systems, either between user and data controller or between related third parties. The most important interest is by far the right of the user to protect his fundamental rights, to keep control on his personal data, to protect his privacy and his right to dignity.
In this context , this paper will look over the right to be forgotten on the internet, by focusing on the particularity of the information ecosystem, and the connotations, implications and foundations of this right.

Introduction2 .
The Information ecosystem3 ..
Two Worlds: different approaches3 .

Are we approving this invasion?4 .
Adhesion Contract: I agree6 .
Serious Social threats: Discrimination7 .
Privacy: Grounding the right to be forgotten8 .
A concept with many connotations11 .
The right to oblivion11 .
Information deletion: Forgetting and erasing11 .
Removing personal data: Re-writing history?14 .
Social forgetfulness: A tool to move on16 .
A proper context 17
The right to be forgotten: Controlling Data19 .
European Directive19 .
Court of Justice of the European Union21 .
New General Data Protection Regulation" (GDPR): Updating24 .
Global right 26
Lebanon: Lack of specific legislation and efficient mechanisms27 .
Conclusion28 .

Introduction

New versatile challenges are emerging with the increasing dependency on Information and communication technologies, and the advancement of their use in processing personal data, in a variety of public and private sectors. new developments in medical research and care, telecommunications, advanced transportation systems and financial transfers, etc... have dramatically increased the level of information collected on each individual. Alternatively, exchanging and transferring data across boundaries are becoming crucial for commercial, financial and governmental activities.

Modern technology of communication is accelerating the erosion of some individuals' rights and misbalancing the interests at stake for the benefit of the new powers of the Cyber space, as well as, for the advantage of governments' increased surveillance. With the internet of things, mobile phones, the desktop, the cloud, practice of information sharing, social Medias, as well as the artificial intelligence, serious threats and sudden risks are upon privacy and security.

ICTs have created new principles; such the openness of the internet and the free flow of information, and new rights; such the access to the Internet and the access to information. Nevertheless, they have shaken up the system of existing rights, and raised a lot of concern about human rights and fundamental freedoms; such as free speech, movement and privacy. For this reason, protecting personal data is becoming more crucial to ensure development of

digital economy, digital innovation, and the protection of the right to privacy and the related rights it involved; such the right to be forgotten, while fostering the free flow of information, the liberty of expression, and the right to access information.
Moreover, the emerging right to be forgotten in the spotlight, with the review of the Personal Data Protection in Europe, reopen the debate on privacy, and its relation to personal data secretly collected, or unreservedly published on the internet.

The Information ecosystem

Two Worlds: different approaches

Communication online has made us lose control over our personal data, over our identities and the way we are represented online, not only to each other, but also to corporations and governments.
Offline ways of communication and environment are different from online ones. They allow keeping private, injudicious, harming or foolish information, for oneself, for a close circle, or limited number of people, and after a while, they are put aside, providing the needed space for people to move on. Offline, we can prevent information from becoming public, and we can count on those who know it, to abstain from rendering it public. Furthermore, even when some people of the close circle discloses it, its spread cannot be as wide as publishing online, and still has limited extension. Offline, we are, to a large extent, sovereign over our private life, we exercise our right to decide what information we want to withhold or even to forget, much easier and much to our convenience.
With the continuous invention and the ascension of new technological devices, the new potential the ICTs provide to keep, memorize and process personal information, people are globally and indefinitely exposed, through personal information they have already published themselves. E- mail archives, browsing history, searches, are continuously pouring easily accessible personal data on the internet, on Android and I Phone. this data constitutes valuable assets for corporations; such as Amazon and E-bay.
However, Many individuals would choose to remove collected data about them from information systems, because this data could be inopportune, irrelevant, or unflattering. And People would like to erase and take such data far away, from public exposure, because it could remind them about some embarrassing or sad situations, they want to forget[1].
So, if there is no legitimate reason for keeping it, the data shall be removed. And, that is the core provision of the right to be forgotten. That's why, the right to be forgotten is said to be mainly about reloading control over personal data, and the way digital identities are traded and represented online.
There is a need to manage the side effects of global, instant and perpetual access to information, that threatens the right to be left alone, when people do feel like it, or the right to

keep privacy from prowlers and snoopers. In this context, the "right to be forgotten" shall act as a safeguard of the right to privacy, as well as of the person's control on his information, and his right to decide what information about him shall be exposed. It also seems like a must to secure the right of a person to protect his reputation, manage his image, and defend his dignity and personality.
For Viviane Reding, the European Commissioner for Justice, Fundamental Rights and Citizenship, this right is: "a modest expansion of existing data privacy rights[2]".

Are we approving this invasion?

In information Society, the anxiety of being profiled, tracked, and surveyed, coincides sometimes with deliberate disclosure of private or even sensitive information. An increasing amount of users' personal data is captured by large online corporations; such as Google and Social Medias, deeply involved in Big Data Technologies, which are intended to help them adjust and respond to changes in customer preferences, market conditions, competition, and other variety of operations. To gain constant awareness and be able to act immediately, online businesses collect, store and process big data in real time, to ensure continuous access. And, while competing to dominate the market, they are merging, affiliating, acquiring, and hence getting more powerful and able to enforce their own conditions on Internet users, in return of their services.
Internet and smart phone users cannot visit a website or use an application, without eventually being asked to agree a listed set of "Terms and Conditions." Whether it is registering for a new social media account, magazines, newsletter, or just trying to get to bank statements, all users have clicked on a button bearing the word "I agree". They may be binding themselves to legally enforceable contracts, with the online service provider.
In the Big Data society, governments are more and more dependent on ICTs to accomplish their traditional role and duties, which makes citizens adhering to these policies look like implicitly have gave up on their privacy, even when they are not internet users. As a matter of fact, personal data is processed in huge public data bases, and collected by surveillance devices; such the ones used in monitoring the traffic or buildings security.
On the other hand, in digital economy's era, personal data has become an important resource, for every corporation, either involved or not, in internet business. It's a unique asset and has great value, not only for the person who created it, but also for creating services that can be rendered online, as well as, offline. On the internet, people are offered 'free' services in return for the exploitation of personal data. This is the business model of any company offering free services, online. Customers are the corporations and the advertisers who buy this data, and use it to target potential clients more efficiently.
According to the broad definition adopted by the EU Data Protection Directive (95/46/EC), "personal data" means any information relating to an identified or identifiable natural person,

described as the Data Subject. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
In principle, it covers any information that relates to an identifiable, living individual; such as a person's full name, a combination of identification elements; such as physical characteristics, pseudonyms occupation, address etc.
Hence, it's what allows determining, locating, following or tracking physically or morally, any given person.
In this context, the question is: have users given the companies permission to harvest their personal data, and sell it to their customers? If so, what are the limits? Do users read privacy policies on how their personal data shall be used, or published by Social Medias. Most of online users don't. So, how can this consent be considered?

Adhesion Contract: I agree

The consent of a user is considered according to the agreement he gives upon accepting conditions or rules of a software or applications' use. That can be demonstrated in a variety of ways, either by words or by actions, depending on the circumstances. Some service providers require users to click an "I Agree" button to show that they agree to a set of terms, whereas other service providers consider the simple use of their website, as a user "agreement" to a set of terms and conditions, hidden somewhere on the site. Yet not all of these techniques are good enough, to create legally binding contracts.
Users in online environment are provided instant access to incredible amount of information. Accordingly, they are not supposed to scroll and rub every inch of a webpage, to find "Terms and Conditions" or "Privacy Policy" 's terms. It goes without saying that the majority of users do not read the legal language that pops up on websites. When users online agree on charts or any other contracts that allow them to use some platforms, applications, or software, they are often neither well informed nor fairly understanding what type of personal data disclosure they consent to. Moreover, people are not expected to understand what can be disclosed through Artificial Intelligence or Data mining techniques, used to process their personal data, when screening or profiling them, for example.
And, even when the long confusing charts contain all the needed information, in very well crafted details, they are still nothing but "adhesion contracts", where the users are practically unable to refuse, or to modify the agreement conditions.
Referring to the Lebanese law of contracts and obligations dispositions (art. 178....), we note that in a contract between two people, there is an offer and acceptance, an intention to create a legally binding agreement, a price paid, a legal capacity to enter a contract of one own free will, and proper understanding and consent of what is involved. Any coercion, false statements, undue influence or unconscionable dealings, could make a contract illegal and void.

Accordingly, the click wrap, as well as the browser wrap agreement, lack clear intention to create legally binding agreement, proper understanding and consent. Moreover, they can be plagued by coercion, undue influence, and unconscionable dealings, when the user cannot modify the terms and conditions of use.

Serious Social threats: Discrimination

Exposing personal data represents potential dangers for individuals and societies that may include: profiling, data mining, identity theft, attacks on infrastructure and IS, personal attack, violence, economic loss, commercial and personal blackmail. Moreover, it may cause discrimination when used by those who are in charge of recruitment, in the public and private sectors.

Employers screen Social networks, online search engines, as well as, credit and criminal backgrounds checking, in hiring. This instance is empirically confirmed; employers are background checking for their employees or applicants, with felony or certain misdemeanor convictions, even though they won't be able to license them in many countries where they operate, because the law will consider them as discriminatory[3].

The results of a research survey, conducted in 2012, by the "Society for Human Resource Management" (SHRM), to understand how Employee in the U.S.[4] are dealing with uncertainty, revealed annoying facts about the repercussions of the "no right to be forgotten", at the hiring process level.

As a matter of fact, while running background checks, on the internet, employers can access Stored collected personal data, that may include, not only undesirable pattern of behave; such those we post on Social networks, but also the content of criminal records. Likewise, the door is open to discrimination in the hiring process, when revealing the provisions of a declaration of bankruptcy or default judgment of a felony.

People's past, old, outdated and not applying to today behavior, still haunting them, when applying for jobs.

Profiles on the net, reveal personal data, all along with the sensitive one.

Some people formerly convicted, fail to find work, because of their record. This is true, not only for the private sector, where employers reject applicants with criminal past, but also, for the public sector, where laws and licensing rules, clearly state the presentation of clean record.

Habib[5], convicted for buying stolen goods, cannot find a job, four years later because of his record, despite the fact that he was jailed for two years. Samir, who lives abroad asked for a record to discover his own stating he had resisted a policeman, four years before leaving Lebanon, and that he won't be hired because of this.

Privacy: Grounding the right to be forgotten

Privacy is a civil liberty directly related to individuals' freedom, dignity and integrity. It constitutes the corner stone of the ability to exercise many civil liberties and fundamental rights; such as the liberty of opinion, and the freedom of expression. The basic international law framework for the right to privacy, which extends to cyberspace, is created through provisions of international, regional and national legislations, declarations, conventions and treaties.

The Article 12 of the Universal Declaration of Human Rights recognizes privacy as a fundamental human right. According to this declaration, no one shall be subjected to arbitrary interference with one's privacy, family, home or correspondence, and everyone has the right to the protection of law, against such interference or attacks. Article 17 of the International Covenant on Civil and Political Rights, states that: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to unlawful attacks on his honor and reputation, and, consequently, everyone has the right to the protection of the law against such interference or attacks.

In seeking balance between the right to privacy and freedom of expression, article 19 states that everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. The only restrictions to this right may be allowed according to the law, and where they are necessary to ensure respect of the rights or reputations of others; the protection of national security or of public order or of public health or morals.

The right of privacy can be defined as the right to be free from government secret surveillance, coercion, intimidation or interference. It is also the right to decide what information to reveal about his private affairs, habits, mode of living, health condition, occupation, residence, conviction, movement, preferences, political affiliation, family matters, communications and conversations. And, while the U.S.A. constitution does not explicitly mention a "right to privacy", it recognizes the right of individuals to retain some rights, even if not stated in the constitution[6]. Hence, some states' Constitutions[7] have explicit provisions relating to a right to privacy. in 2014, Missouri became the first state to provide "explicit constitutional protection (art. I, § 15) from unreasonable searches and seizures for *electronic* communications or data, such as that found on cell phones and other electronic devices"[8].

This right means people have the right to lead their life in a reasonable manner of seclusion from public scrutiny, be it a neighbor or a public authority. According to Brandies, who presented the right to privacy as the right to be left alone, "privacy is "the most comprehensive of rights and the … most valued by civilized men [9]". The USA constitution goes further in its fifth amendment, to recognize the criminal suspects the right to keep secret, any incriminating

evidence that might help the government obtain a conviction against them.
Almost every country in the world recognizes a constitutional right to privacy online.
In addition to some new constitutions (South Africa), many European countries have approved laws to regulate surveillance of personal data, and protect citizens' privacy[10]. The UN has supported protection of privacy by backing up a draft resolution[11], prepared by Brazil and Germany, and titled "The right to privacy in the digital age[12]".
In the digital age, the concept is fused with Data Protection, which interprets privacy in terms of management of personal information. Privacy is considered in a new light, related to the explosion of pouring personal data in cyberspace, and the high level of connectivity, that turns each individual into a "sensor for the world intelligence community[13]."
Yet, there is no global consensus on what can be considered as adequate protection of privacy. Principles of privacy protection are stated by many regional and international instruments, such as:
- The 1980 "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," issued by the Organization for Economic Cooperation and Development, and that apply to personal data that poses a danger to privacy and individual liberties, because of their nature, or the manner in which they are processed and used, either in public or private sectors.
- The 1981 "Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data", issued by The Council of Europe
- The 1989 "Guidelines on the Use of Computerized Personal Data Flow", issued by the council of Europe
- The 1999 United Nations "Guidelines for the Regulation of Computerized Personal Data Files"
These guidelines establish principles of minimum privacy guarantees for personal information, at all stages of its processing operations (collection, storage, dissemination, use, transfer etc…). They also recognize the right of the individual to access its personal data, to update it, to be informed on the methods and the objectives of the data collection's operations.
Moreover, they establish the right of the individual to have his data destroyed, after the purpose of its collection and processing is achieved, which supports the right to be forgotten on the net.

A concept with many connotations

There is no simple answer to the question: what is the right to be forgotten? Because this right is not only new, but rather a complex concept, despite the fact that it has been mentioned by a variety of legal expressions; such as the right to oblivion, the right to ask for information deletion, and social forgetfulness. All these expressions are closely related to absence of reminder that may provide knowledge, or bring memories back, and which is: "information".

The right to oblivion

According to Merriam Webster Dictionary, oblivion simple definition is: "the state of something that is not remembered, used, or thought about any more", or even:" "the state of being destroyed" while the full definition is: "lacking remembrance, memory, or mindful attention, or lacking active conscious knowledge or awareness".
At the legal level, the right to oblivion is related to the justice's rehabilitation system, that aims to protect one's reputation and personality's rights. In French system, “Le droit à l'oubli” is double - edged. It means avoiding being confronted with the past, as well as, the right not to be confronted with it, by giving the data subject, the control of already published data.
Accordingly, we can say that the right to be forgotten may find its roots in the French legal system, where the law recognizes the right of oblivion for convicted people, after they serve their punishment and prison time.

Information deletion: Forgetting and erasing

On the other hand, the right to ask for information deletion is established by the data protection legislation, that imposes either deleting or anonymizing irrelevant data, or after the purpose for which this latter was collected is achieved.
This right to ask for information deletion or erasure, could also find its foundation in article 8[14] of the Convention for the Protection of Individuals, with regard to Automatic Processing of Personal Data 1981, as additional safeguards for the data subject.
The convention recognizes the right to erasure of inaccurate, outdated, excessive, or kept longer than it is required for the purposes for which those data are stored, according to the provisions of its articles 5[15] and 6[16].

In online environment, information is there to stay, and to come out on search operations. That’s why it’s said: the internet doesn’t forget[17]. And it seems that this perception prevails, despite the fact that the web is volatile, and valuable information keep disappearing. Hence, the right to be forgotten online, means not only the right to oblivion, but also the right to remove the data that one's doesn't want to go out in search operation's results, when his name, or any other personal data about him, is used as a keyword.
But this erasure made some see this right as absurd[18], not only because it means asking search engines to remove stories they just indexed to be accessible, but also because it looks like asking libraries to remove news stories about individuals from their archives.
“the right to erasure” is intended to grant people control over their own personal data, in facing “Big Data” phenomenon, while the right to be forgotten” is intended to exercise the right to privacy, protect reputation and identity in the online society. It's directly related to one's "right to privacy".
The right "to erasure" looks like a condition to enjoy the right to be forgotten. It gives the data

subject the right to limit and stop unlawful use of his personal data. In practice, it means removing personal data that has been posted, or released for automated processing, which is a must to start forgetting process.
According to 1981 convention, as well as to the new proposal[19], the right to be forgotten, in practice, is about deleting personal data, delisting, or making it disappear from search results, which makes it an answer to the rising damages of the internet's everlasting memory, on personal reputations and private lives.
According to the working group 29 (WP29), the erasure on search engine, doesn't affect the original information that could stay accessible using search terms, other than the person's personal name, pseudonyms or nicknames.
In 1989, The right to be forgotten was directly connected to the right to demand erasure of personal data, by the committee of experts on data protection, in the context of data collected and obtained through telemetry, that should be erased after a certain time[20].
When Google introduced the web-form for personal information removal, the press reported tens of thousands of requests, many of which were sent by criminals, pedophiles, dodgy doctors, and politicians. But, In the information society, personal information on the internet are not, anymore, the concern of criminals, but also of ordinary people, with no criminal records at all.
According to the EU law, every citizen or resident of an EU state, is entitled to request delisting or erasure, from online search engine.

Removing personal data: Re-writing history?

The data that people can ask to remove is supposed to be the "personal data" that they have provided themselves, and not the data that have been published by the media, otherwise individuals would be controlling, not only their online reputation through the data they put online, but also the references on the internet.
Building on this fact, once online, information should stay online, except when it's unlawful under copyright or criminal law.
According to Peter Fleischer, the chief privacy counsel of Google, it is entirely unobjectionable to allow internet users to delete what they have posted online; such a photo or a comment, while it becomes controversial to ask search engine to remove this data after it had gone viral and posted by other users; such as the internet user's friends, especially that it means to ask each one of them for their consent[21]. Moreover, things become more divisive when users ask to remove what has been posted about them by others, since it means that the search engine is to play the role of a judge, by deciding if this content is harmful, or privacy invasive. And here, it goes without saying, how sensitive is the situation, especially that it involves identifying any relevant third parties, and securing the takedown of the content, to avoid a fine. And, the situation could get more complicated, when the third party is able to prove, according to the

regulation, that the retention of data is necessary, either for the exercise of the right of freedom of expression, or for journalistic purposes.
For that reason, recognition of this right could lead to a significant impact on the openness of the internet, if a clash occurs between mutual conceptions of the convenient balance between constitutional rights; such as the "Free Speech" in the United states, and the "Right of Privacy" in the European countries.
The public interest could also be at stake, if people were denied the right to access information about public figures, as well as professionals, and criminals. This is true, if these latter, would be recognized the right to re-write their history, and ask for erasure of information revealing their past.
In W?grzynowski and Smolczewski v Poland, the European Court of Human Rights[22] tackled balancing issues between freedom of expression and the right to private life, in the context of the right to be forgotten, and noted that "particularly strong reasons must be provided for any measure limiting access to information, which the public has the right to receive".
Furthermore, it recognized that the right of reputation places limit to the right to access information, but was skeptical about rewriting history by judicial authorities. This skepticism of the right to be forgotten, can be traced to a report of the committee of experts on data protection, on 1990, entitled " Data protection and the media (1990)[23]", which criticized the right of the data subject and wondered if giving him the right to rectify " erroneous reports which are stored in electronic archives", will escalate in the danger of giving him the ability to re-write history.
This issue was among many points of the Google Spain v Costeja ruling, that were addressed by the European data protection authorities (DPAs) assembled in the Article 29 Working Party (WP29), On November 26, 2014. The WP29, acknowledged the need of a fair balance between fundamental rights and the implicated interests, to limit the impact of delisting on the right to access to information, and the freedom of expression. It stated the delisting inappropriate when the interest of the public overrides the rights of the data subject, once this latter plays a role in public life[24].As a matter of fact, there is an urgent need to define this right, as well as the right to privacy, as it could grow to be a serious source of liabilities for search engines, which fails to remove personal information posted by people who regret them, and after they are already widely distributed[25].
While companies should abstain from the misuse or unpermitted collection and retention of data, consumers have to be cautious when they allow access to their data, and demand better protection.

Social forgetfulness: A tool to move on

Far from the internet, some people were faced with the difficulty to escape their regrettable unwanted past, because of some criminal actions they have committed, recorded and

published by the authorities in charge. Accordingly, traditional legislations found the solution in recognizing individuals the right to rehabilitation, after serving their time and a certain number of years defined according to the crime's nature and classification; such as misdemeanor or felony.

Social forgetfulness has been seen as a mean to bring a willing person back into the community[26], and legislations have previewed some legal mechanisms that recognize pardon for the offender.

At a general level, a form of forgetting is amnesty. It has been used since old times, in Greek, and stated by Roman law, since the 4th century B.C. to end the civil war[27]. Since, amnesty has always been seen as a tool of forgetting some criminal acts, committed by some members of the society, in order to foster reconciliation, and allow a nation to compromise and reunite. Modern constitutions recognize the power to grant amnesty, either for the legislative bodies or for the executive ones. On some occasions, amnesties could be initiate as part of legislations. likewise, In 1991, the Lebanese government and parliament drafted and approved an Amnesty Law[28] against all crimes committed during the war, and they marketed it as a way of reconciliation.

In the time of manual processing of individuals' personal data, criminal records was proper mean to render public the criminal actions, and to ensure protection of society against criminals individuals. And, when rehabilitated, records were kept, but convicted individuals were entitled to have a clear criminal record. In the internet time, there is this need to keep this right, and that's where comes the right to have old information kept hidden from public eyes, when it is not serving any purpose that can be considered of interest, neither for society, nor for individuals.

According to a UK Act[29], "a rehabilitated person shall be treated for all purposes in law, as a person who has not committed or been charged with, or prosecuted for, or convicted of, or sentenced for the offence or offences which were the subject of that conviction; and, notwithstanding the provisions of any other enactment or rule of law to the contrary" Moreover, on July 2003, "Principles concerning the provision of information through the media in relation to criminal proceedings, " found in Declaration and Recommendations of the Committee of Ministers to member states[30], show considerations of personality right that forbid publication of criminal records. These considerations allow a restriction on the freedom of information, for the stake of the convicted criminal, when the interest of reintegration outweighs the interest of society to be informed.

In Lebanon, According to articles 159 and 160 of the penal code, and the criminal record law, rehabilitation is a right that can be obtained, when certain conditions are met. Physically, this operation consists in purging the criminal record. Effectively, the privacy claim applies on

information that is public, to a certain degree, and most of all for the information held by the authorities in charge of security.

A proper context

According to the definition given to a legal right, as a power, privilege, demand or claim possessed by a particular person by virtue of law, corresponding to a legal duty imposed on other, the right to be forgotten gives the individual the right to enjoy his privacy, and keep his life secluded and safe, from any unjustified interference of others, in his past life.
On the other hand, the others are under the obligation to abstain from any trespass of this right, which is related to the right of privacy, that grows out of the nature of the individuals as human beings.
Over time, even the accurate information loses its proper significance, weight and context, and could lead to identity distortion by the internet. So, the right to be forgotten, may seem like a right of a proper context that helps protect individuals' identities, especially with the potential of the internet to bring out the archive of a person.
This right can be defined as "the right to silence on past events in life that are no longer occurring.[31]" And hence, may seem not like a right in itself, but rather like a restatement of other rights that are recognized by the law; such as the right to privacy, or the right to protect one's reputation and dignity.
Nevertheless, this right should be distinguished from the right to privacy, because of their different scope. The first applies on information that is not publicly known, whereas the second involves removing information that was publicly known, at a certain time, and prohibiting access to it.
From a legal perspective, this right positions the subject data as the owner of the information and data generated by his online activities. It offers him a measure of control over his personal data that is equipped with enforcement mechanisms, when this control is violated.
However, Personal data is not concretely in possession of a given party, neither exclusively retained by it, since there is not just one site that may have a user’s personal data, but a multitude of third parties and mirror sites.
Hence, Personal data is an intangible asset that makes the enforcement of a right of ownership difficult to implement, and raises many basic legal questions; such as the one about the possession of an intangible asset, subject to sharing, even when it is meant to be kept secret, sometimes. On the other hand, there are the problems of exercising control over this data, that can be easily replicated, disseminated and shared.

The right to be forgotten: Controlling Data

The article 12 of the 1995 Data Protection Directive, has already underpinned the principle of the right to be forgotten, by recognizing the deletion of the data when it is no longer necessary.

Accordingly, a person can ask for his data to be removed from the search engine online, when this information is inaccurate, inadequate, irrelevant, or excessive[32], for the original purpose of the processing.
The proof of the data necessity must be provided by the responsible of personal data processing. In this context, the European commission has proposed to reverse the burden of proof, and ask the responsible of the data processing to prove it is still necessary. This obligation can be understood in the light of its practical roots, lying in the difficulties internet users face to erase unwanted personal information, on the internet.
Moreover, the European Directive grants the individuals, whose personal data have been processed, the right to require the controller to rectify, erase, or block any data the processing of which does not comply with the provisions of the Directive, as well as to object to the processing of data relating to them. According to Article 2(d) Directive 95/46/EC, the"controller" of data, is the natural or legal person, public authority, agency or any other body which alone or jointly with others, determines the purposes and means of personal data processing.

European Directive

This right can also found its foundation in The actual European directive, requiring Member States to legislate in a way that ensure, personal data processing is fair and lawful(art.6.1.a). According to article 2(b) "processing of personal data" is "any operation or set of operations which is performed upon personal data, whether or not by automatic means". A non-exhaustive list of such processing's operations includes collecting, retrieving, recording, organizing, disclosing and making available personal data .
Moreover, the controller of the data has the obligation to ensure that it is only collected for specified, explicit and legitimate purposes (art.6.1.b), that no more is collected than what is necessary for these stated purposes(art.6.1.c) crucially that the data are accurate and kept up to date, taking every reasonable step to ensure rectification or erasure if it is not(art.6.1.e) and that the data are only kept for as long as necessary (art.2.b).
The 1981 convention, and the current EU Data Protection Directive 95/46/EC were adopted, long before the emergence of the cyberspace that aggravated risks and threats to privacy, rendered even more overwhelming with the appearance of social networks, the unprecedented spread of smart phones and mobiles' use, the cloud computing techniques, the internet of things, web-tracking technologies, as well as without consideration of the globalization phenomenon[33].
The 1995 EU Data Protection Directive, allows collection of Personal data for specific, explicit, and legitimate purposes, and prohibits holding any data that is not up-to-date, relevant and accurate. And, EU member states are obliged to stop transfer of this data abroad[34], in absence of equivalent measures, that allow data protection and citizens ‘rights to access, protect,

modify, and deny the right to use of their data, by third party.
Hence, to allow cross board data flow to U.S.A, where there is no such level of adequate protection, the EU reached the “safe harbor agreement” with the former. This agreement allows some US companies, to collect data about EU citizens, in case they proof their engagement to ensure data protection meets EU standards. These companies, should inform EU citizens, on how their data are processed and used, and recognize their rights to access, withhold, and modify their data. Nevertheless, in a landmark verdict " the Court of Justice of the European Union declared that:" the Commission’s US Safe Harbor Decision is invalid"[35].
As a matter of fact, after the Edward Snowden’s revelations, in 2013, on the complicity between USA based hi-tech and telecoms companies and government intelligence agency, allowing a massive access to personal data, an Austrian lawyer, Maximilian Schrems, complained before the Irish Data Protection Commissioner(DPC), that Facebook was violating his privacy by retaining his data in the US, including material he had himself deleted.
The Irish Data Protection Commissioner (DPC), rejected the complaint and declared having found no case. Schrems filed a complaint before the high court of Ireland, which referred the case to the court of justice of the European Union (CJEU), On 18 June 2014[36].
The high court of Europe observed that, the Commission has merely examined the safe harbor scheme, and didn't examine, as it should have done, if the United States was ensuring a level of protection of fundamental rights, equivalent to that guaranteed within the EU, under the directive read in the light of the Charter.
It considered the indiscriminate interception of communications, to be a violation of fundamental rights, by stating that "legislation permitting the public authorities to have access, on a generalized basis to the content of electronic communications, must be regarded as compromising the essence of the fundamental right to respect for private life". According to this verdict, masses of Europeans 'personal data transfer to the USA, are in breach with the fundamental right to data protection, because many digital operators do not provide customers with protection from state surveillance.
The European Union Data Protection Directive of 1995, regulates the free movement of personal data, and imposes the adoption of its provisions into domestic law, while allowing individual EU countries, to exercise their own approaches to implementation. Data subjects shall be guaranteed the right to know where the data originated, the right to have inaccurate data corrected, the right of appeal in the case of unlawful processing, and the right to deny permission to use data under certain circumstances.

Court of Justice of the European Union

In a recent judgment (Case C-131/12, 13 May 2014), the CJEU laid down an important presumption in favor of the rights to privacy and the protection of personal data, by interpreting article 12 of the 1995 European Directive, as applying to data on the web,

accessible through search engine. The court hold up that these rights have like a priority on other rights. Hence, they 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, and, particularly, the freedom of expression.

This decision is a landmark. It explicitly affirmed the existence of a right to be forgotten in the EU, as a matter of principle. And, it clearly stated that the erasure of irrelevant or unwanted data, is a necessary part of forgetting.

Upon this, it decided that a person has the right, to have his personal data removed from the index, used in search. This means, the personal data may no longer be made available to the general public, by its inclusion in the list of search results, when they are tailored to an individual's name through the search engine, because they allow to establish a more or less detailed profile of him, by providing a vast number of aspects of his private life, and which cannot be easily obtained or interconnected without the search engine.
To reach this judgment, the court interpreted the provisions of the directive 95, in the light of fundamental rights, because it seeks to protect fundamental rights and, particularly, rights relating to privacy, as it is stated in articles 7 and 8.It endorsed the complaint against Google, stating that search engine operators had a direct obligation to erase the data, when this later is able to compromise the fundamental right to data protection and the dignity of persons, which included the person's desire that such data not to be known to third parties.

In the case, a Spanish citizen Mr. Costeja Gonzalez sought to obtain an order to the effect that information about auction notices for the recovery of social debts he has owed 16 years earlier, which appeared in a newspaper and on Google search results be altered, deleted, or protected, and that Google should either delete or conceal the links to those pages.
However, we should notice that this decision is not about personal data willingly posted online, but rather about information originating from public records, which is a newspaper, and which is considered just like other public sources, television and other media. Also, this information is accurate, and legal. it was published upon order of the minister of Labor, to ensure wide publicity of the auction and, hence, to guarantee participations of the largest number of bidders.
According to this ruling, the individuals were recognized the right to directly address search engine operators, to ask them erase data about them, on the basis that they do wish to be forgotten. In this case, the court considered the search engine Google as a data controller, responsible to take the needed measures to administer the requests of data erasure, and,

accordingly, to play the role of the court, when deciding which requests shall be positively answered. The court has extended Directive to consider the search engine a "controller", while it does not process data, and cannot be considered aware of the personal data existence. Moreover, he is not the one who has defined the objectives for the processing operation. Thus, the court recognized the data subject has the right to ask rectification or erasure from the operator of a search engine, like he can do it from the "controller" .

According to the Directive, A controller, shall at least process data, which is not true for a search engine. Article (2.d) of the Directive defines the controller as following"...the natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;"

Alternatively, the court gave a broad interpretation of the Directive's territorial reach, by extending it to cover organizations outside Europe. It considered Google activities in Spain into the territorial scope of the Directive, despite the fact that these activities are not about data processing.
On the other hand, In a clear effort to capture more US companies, than it is done with the actual Directive and 108 convention, the new regulation (GDPR) extends its territorial scope, to include personal data processing by controllers or processors established in the EU, or processing of personal data of subjects based in the EU, where the processing relates to goods or services offered to those data subjects, or the monitoring of their behavior[37].
Removing data online doesn't mean removing it from official records or newspapers, which had publish it, and that is true for the Mr. Costeja Gonzalez' case, whose name appears in many articles, as well as in reports about the case, or even in the minister and auctions' records.

New General Data Protection Regulation" (GDPR): Updating

The right to be forgotten has been codified as part of a broad new proposed data protection regulation in Europe. This proposal is built on the already existing obligation of data controllers to stop processing personal data when the legitimate ground and purpose no longer exist.
The European Parliament and the Council of Ministers have been working on a proposal for a new regulation of personal data protection, released in January 2012, and entitled "new General Data Protection Regulation" (GDPR). This proposal aims to harmonize data protection rules across the EU and is part of a package that also includes a draft Directive on the processing of personal data by public bodies, for various justice and crime prevention purposes[38].

This latter ensures an enhanced level of data protection, as well as far strong rights, starting at the first step of collection till the collection's purpose and use. The Data controllers have the obligation to be more transparent on how they will be using the collected personal data, especially, when it is shared. For this purpose, they have to provide more details about their privacy policy, in clear and plain language, that can be understood by data subject, must have the unambiguous consent by the data subject, while granting him easier access to his data. A special attention is given to personal data collected from the data subject when he was a child, by recognizing him a right "to erasure" and a right "to be forgotten", requiring the service provider to erase this personal data without delay.
In May 2014, the European Parliament approved a version of the text for the GDPR, and The European Council finalized its text, in June 2015.
Despite the fact that the new Regulation uses the same language to talk about data protection; such as: personal data, processing, data controller, and data subject, many of the terms' definitions have been expanded to make controller and processor tasks more tedious, in their quest to abide by the rules.
As for the data's subject consent, for example, The GDPR is tightening the circumstances where controllers may rely on implied consent. According to Article 4 (8), consent is: “any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed". Moreover, dispositions are hardened by recognizing the data subject the right to withdraw his consent, at any time.
In the light of these changes, data controllers processing personal data according to data subjects' consent, shall be reviewing their ways for obtaining this latter, especially that, they will bear the burden of proof of this consent[39].

According to the actual Directive provisions (art.6.1.d), an individual has the right to ask the data controller, a rectification or erasure of the inaccurate or incomplete information. The controller has the same obligation, when the data is slanderous or disrespect civil rights.

The GDPR codifies the right to be forgotten in its Article 17, to give more control for the data subject over its personal data. The first paragraph 17(1) contains the right to erasure for the data subject, and the obligation of the data controller to erase and to abstain from further dissemination. According to this right, the data controller has the obligation to erase information where it is no longer necessary, for the purpose for which it was collected, where the data subject withdraws consent, or where they object to processing. In paragraph 2, there is no right to erasure or obligation to stop processing, but rather another obligation that lays on the processor the obligation to take reasonable steps to inform third parties that the data

subject has requested erasure, if the personal data has been published on the internet.
This paragraph establishes an obligation of result, with the regard to the information of third parties that were authorized to publish this data, that the data subject has requested erasure of such data. The application of this obligation is depending on the controller liability of third parties publishing. This is true each time the controller gives third parties his authorization to publish this data. According to the actual Directive 95/46/EC, article 14 recognizes the data subject the right to object to processing his personal data, even when this operation has a legitimate ground. He can oblige the controller to stop processing his personal data, by proving specific circumstances that constitute "compelling legitimate background". While under the (NGR), the burden of proof is on the data processors and controllers, who have to proof the need to keep processing data. Actually, the added value of this article relates to published information.
According to many European commission documents and speeches of Commissioner Reding, this right is intended to cope with privacy risks on line, by allowing individuals, to control their own data on the internet.

Global right

To put the right to be forgotten in context, as a concept that relates to the protection of Personal Data, aiming to avoid privacy harms done by new forms of digital publicity on search engine and social medias, we should be aware that the global nature of the internet, has a decisive impact on the effectiveness of this right. Cyberspace, where no real frontier exists, allows the clash of different legal systems regarding the concepts of "freedom of expression" and "personal data**".** For example, the Communications Decency Act of 1996 (CDA), also known by some legislators as the "Great Internet Sex Panic of 1995", enacted as a mean to prevent the transmission of indecent and patently offensive materials to minors over the Internet[40], protects intermediaries from all liability for the posting of third parties, through section 23o which states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information, provided by another information content provider" (47 U.S.C. § 230) .
Moreover, the internet is not a “public space” where a given country may extend its sovereignty, but rather an algebraic representation of privately owned services.
On the other hand, this right has raised serious issue about the implementation of the decision taken by the Court of the European Union, especially between countries with different legal priorities; such as the EU and the USA. the principle of sovereignty denies the right of a country to control what should be seen or published in another country, especially that it influences the freedom of expression, and the right to access information, as well as the free flow of information. Nevertheless, according to the "extra territorial effects" of national legislations, corporations and search engines will be obliged to implement national decision recognizing an

individual's right to be forgotten, and, consequently, erase the PD or PI personal information wherever this data is.
In an answer to Google objections, the French National Commission of Informatics and liberties (CNIL), has considered that this argument is in part political, and that the legal reasoning imposes the application of the right on all Google extensions. Actually, the new regulation aims to ensure European citizens the same level of protection, no matter where the processing of their personal information takes place.

Lebanon: Lack of specific legislation and efficient mechanisms

According to the constitution preamble of 1990, Lebanon, a founding and active member of the United Nations Organization, abides by its covenants and by the Universal Declaration of Human Rights. And, The Government shall embody these principles in all fields and areas without exception.
Nevertheless, Lebanon is currently failing to constitutionally uphold the right to privacy, to adopt a convenient legal framework to protect personal data, and to ensure legality of communications surveillance, pursuant to its international human rights engagements.
the constitution recognizes Individual liberty as guaranteed and protected by law (art.8), freedom of expression and freedom of the press, (art.13), and the traditional form of privacy through inviolability of the residence (art.14). But this recognition cannot afford to protect privacy online, even if this latter is defined as seclusion from public publicity, because physical seclusion is a clear concept, that becomes complicated if applied to intangible asset like information and personal data.
The Information privacy is recognized by sectoral legislations, for banks' accounts, lawyers and doctors, under the label of professional secrecy, while privacy of communications carried out by all means of communication is uphold according to legal dispositions of Law No. 140 (Telecommunication Interception Act of 27 October 1999). The Lebanese constitution supports Territorial form of privacy, by setting limits to intrusion into the domestic and other environments; such as the workplace or public space.
Lebanon has no legislation on "Personal Data Protection", despite the emerging initiatives of the e-government, the Unique ID, the biometric passport, and the E-transaction bill which, in its current state, would allow for warrantless search and seizure of financial, managerial, and electronic files, including hard drives, and computers. As a matter of fact, The United Nations International Independent Investigation Commission (UNIIIC), and the Special Tribunal for Lebanon (STL), had have unregulated access to personal data of Lebanese citizens from many sources: educational, government, medical, and mobile phone records. Moreover, internet service providers are requested to track Lebanese citizens activities on the net, by an order issued by the Public Prosecutor’s office, on June 2013.
An order issued by the public prosecutor's office, issued on June 7, 2013, establishes a practice

of tracking internet users, by landline and wireless service providers. These latter have an obligation to store the online traffic, for at least one year[41].
Recently, the Lebanese parliament has listed on its agenda a draft law, on the access to information, while still discussing another one on E-transactions and Personal data Protection. This latter, has previewed the principle of personal data protection, in some articles, under chapter 5, with no clear or efficient mechanisms, on the how to implement this protection.

Conclusion

It goes without saying, that the discussion is still open, and that the struggle to protect privacy and recognize the right to be forgotten, is unfolding within a digital ecosystem characterized by surveillance. The right to access, process, analyze, disclose, seek, find, transform, and distribute information, must be reconciled with the equal right and need to be left alone. Government must recognize the innate danger in the collection and retention of personal information, that some incidents such as "revenge porn" sharing, or "pictures uploaded" due to poor judgment, can do a lot of harm. They must protect citizens by providing them the needed legal tools, that empower them to protect themselves against corporations commercial practices, as well as, against some types of cybercrime, and illegal surveillance of the public authorities.
At the legal level, the recognition of the right to be forgotten, may afford a higher level of protection for human rights. However, the reach of the obligations enshrined in Articles 7 and 8 of the Charter of human rights shall be defined, and balanced with the need to protect Article 11 of the Charter, recognizing the freedom of expression and information as everyone's right, and as including "freedom to hold opinions", and "to receive and impart information and ideas", without interference by public authority, and regardless of frontiers.
Nevertheless, the right to be forgotten on the internet may be sloppy, when it isn't balanced with the "right to access information" and the "freedom of expression", especially in weighing the interest of the general public in having access to the information. Hence, this right is not intended to cover criminal tracks, by removing damaging or incriminating information; such as corruption, sexual assault, corruption revelation, child pornography, particularly, for those who run for political positions. Anyhow, it should not be, by any mean, used to manipulate or eliminate information that could be prominent for public interest.
To achieve balance between the right to be forgotten and the right to access information, the right to freedom of expression and information that are substantively guaranteed by a fundamental right, legislations should also seek to weigh up protection of fundamental rights with economic interests, as well as, with the right to access information.
Actually, the European Directive[42] does allow Member States, to make an exception to some of its basic rules, on personal data protection, insofar as this would be necessary, in order to reconcile the right to privacy with the freedom of expression and, particularly, with journalistic,

artistic, or literary expression.
A fair balance' between the 'interest' of Internet users in having access to the data in question, 'and the data subject's fundamental rights, should be established.
There is a need, that the data subjects and the website owners or operators, shall be able to understand, where the limits of these rights and responsibility are placed.
Next to this, Information and communications Technologies shall contribute, not only to securing data, but rather to improve the way personal data is handled and processed, so that search engines and data processors apply principles of personal data protection, in a way that may respect the right of a person to privacy, to seclusion and to be forgotten.

---

[1]Caught in the web: case histories of people whose digital past haunts them http://www.theguardian.com/technology/2013/apr/04/web-case-histories-digital-past

[2] - The Right to Be Forgotten. February 13, 2012 64 Stan. L. Rev. Online 88 by Jeffrey Rosen Professor of Law, The George Washington University Legal Affairs Editor, The New Republic http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten

[3] - http://www.eeoc.gov/eeoc/newsroom/release/1-11-12a.cfm
Company's Former Use of Criminal Background Checks Discriminated Based On Race, Agency Found

[4] - http://www.shrm.org/Research/SurveyFindings/Documents/12-0537%202012_jobsatisfaction_fnl_online.pdf
2012 Employee Job Satisfaction and Engagement

[5]http://www.al-akhbar.com/node/22393

[6] - Amendment IX
The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.
https://www.law.cornell.edu/constitution/ninth_amendment

[7] - in 10 states—Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina and Washington—

[8]- http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx

[9]- Defining Privacy
https://www.scu.edu/ethics/privacy/defining-privacy/

[10]- FISA Amendments Act of 2008, Communications Assistance for Law Enforcement Act , in the USA
- Data Protection Act 1998 and Regulation of Investigatory Powers Act (RIPA) in the United Kingdom - Informatics and civil Liberties Act 1978 in France- EU convention of Personal Data Protection, EU Data Retention Directive,

[11]- General Assembly backs right to privacy in digital age
http://www.un.org/apps/news/story.asp?NewsID=46780&Cr=privacy&Cr1=#.UwCw6ThWHZY

[12]- Sixty-eighth session- Third Committee- Agenda item 69 (b) Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms

[13]- Philippe Langlois- founder of the Paris-based company Priority One Security, on agencies' ability to harvest personal data from users of smartphones.
http://www.nytimes.com/2014/01/28/pageoneplus/quotation-of-the-day-for-tuesday-january-28-2014.html?_r=0

[14]- **Article 8 – Additional safeguards for the data subject**
Any person shall be enabled:
a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;
c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set

out in Articles 5 and 6 of this convention;
d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied

[15]**- Article 5 – Quality of data**
Personal data undergoing automatic processing shall be:
a. obtained and processed fairly and lawfully;
b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
d. accurate and, where necessary, kept up to date;
e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

[16]**- Article 6 – Special categories of data**
Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

[17] - "The bad news for anyone who has been outed — the Internet does not have a delete button," says Carmi Levy, an independent technology analyst in London, Ont. http://www.vancouversun.com/sports/Internet+doesn+forget+Managing+disgrace+digital/4992930/story.html#ixzz3RhbcnDMP

[18] -This ruling shows the absurdity of Europe's 'right to be forgotten' law http://www.businessinsider.com/eu-right-to-be-forgotten-law-is-idiotic-2015-8
· Aug. 20, 2015, 2:04 PM

[19] - Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

[20] - Data protection Compilation of Council of Europe texts Directorate General of Human Rights and Legal Affairs Strasbourg, November 2010

https://www.coe.int/t/dghl/standardsetting/dataprotection/dataprotcompil_en.pdf

[21] Peter Fleischer: Privacy...? Foggy thinking about the Right to Oblivion - Wednesday, March 9, 2011
http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html

[22]http://merlin.obs.coe.int/iris/2013/9/article1.en.html

[23] - Data protection and media (1990) Study prepared by the Committee of experts on data protection (CJ-PD) under the authority of the European Committee on Legal Co-operation (CDCJ), Strasbourg 1990
https://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Media_1990.pdf

[24]- GUIDELINES ON THE IMPLEMENTATION OF THE COURT OFJUSTICE OF THE EUROPEAN UNION JUDGMENT ON"GOOGLE SPAIN AND INC V. AGENCIA ESPAÑOLA DEPROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJAGONZÁLEZ" C-131/12- Adopted on 26 November 2014
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

[25]The Myths & Realities Of How The EU's New "Right To Be Forgotten" In Google Works
http://searchengineland.com/eu-right-forgotten-191604

[26]Fordham Urban Law Journal Volume 27, Issue 5 1999 Article 37 Forgiveness and the Criminal Law: Forgiveness Through Medicinal Punishment Dennis M. Cariello∗
http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2033&context=ulj
December 5 2015

[27] - The Oxford Encyclopedia of Ancient Greece and Rome
https://books.google.com.lb/books?id=lNV6-HsUppsC&pg=PA91&lpg=PA91&dq=civil+war+greek+amnesty&source=bl&ots=QoFNmQexvM&sig=CelLQw6MUH_ipq3iIqSKWm3av1o&hl=ar&sa=X&ved=0ahUKEwjys6jds5DLAhWCTBQKHR6rAgUQ6AEILzAD#v=onepage&q=civil%20war%20greek%20amnesty&f=false

[28] Law number 84/91 26 August 1991

[29] - An Act to rehabilitate offenders who have not been reconvicted of any serious offence for periods of years, to penalise the unauthorised disclosure of their previous convictions, to

amend the law of defamation, and for purposes connected therewith.
http://www.legislation.gov.uk/ukpga/1974/53

[30] - ***Ministers' Deputies***- CM Documents- CM(2003)85 12 June 2003- 848 Meeting, 10 July 2003- 5 Media- 5.1 Steering Committee on the Mass Media- Abridged report of the 59th meeting (Strasbourg, 13-16 May 2003)
https://wcd.coe.int/ViewDoc.jsp?id=42101

[31] - computers, privacy and data protection: an element of choice
https://books.google.com.lb/books?id=7iLyulobRg8C&pg=PA90&lpg=PA90&dq=%22the+right+to+silence+on+past+events+in+life+that+are+no+longer+occurring.%22&source=bl&ots=gDSxNBplgK&sig=tzxEeujKNXmymISf2NQJ_VEjx50&hl=ar&sa=X&ved=0ahUKEwjA66Kg1vXKAhUHChoKHfcUC0wQ6AEIMzAD#v=onepage&q=%22the%20right%20to%20silence%20on%20past%20events%20in%20life%20that%20are%20no%20longer%20occurring.%22&f=false

[32]http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

[33] - http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (seen on 1/6/2016)
Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
"During the consultations on the comprehensive approach, a large majority of stakeholders agreed that the general principles remain valid but that there is a need to adapt the current framework in order to better respond to challenges posed by the rapid development of new technologies (particularly online) and increasing globalisation, while maintaining the technological neutrality of the legal framework".

[34]- 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- *Official Journal L 281 , 23/11/1995 P. 0031 - 0050*
- (57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

[35] - Court of Justice of the European Union PRESS RELEASE No 117/15 Luxembourg, 6 October 2015 Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner

http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

[36] - Schrems -v- Data Protection Commissioner [2014] IEHC 310 (18 June 2014) http://www.bailii.org/ie/cases/IEHC/2014/H310.html

[37]- Article 3 Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.
2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:

(a) the offering of goods or services to such data subjects in the Union; or
(b) the monitoring of their behaviour.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

[38]**- Data protection for police and judicial cooperation in criminal matters: Council ready for talks with EP**
http://www.consilium.europa.eu/en/press/press-releases/2015/10/09-data-protection/

[39]According to Article 7: any consent wording must be:"in an intelligible and easily accessible form, using clear and plain language".

[40] - What does CDA stand for?CDA stands for Communication Decency Act http://www.acronymattic.com/Communication-Decency-Act-(CDA).html

[41] - Providers tracking customers' Internet use. : "all landline and wireless internet service providers for homes and companies and from all cafés and stores providing their clients with devices through which they can access the Internet" to "do whatever it takes to activate and save all Internet log files going through their servers and routers, and prepare a periodical backup copy to save these files from being lost, for at least one year" https://now.mmedia.me/lb/en/reportsfeatures/523209-523209-523209-providers-tracking-customers-internet-use

[42]Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data