Gottfried Wilhelm Leibniz Universität Hannover

Universitetet I Oslo

EULISP 2017/2018 – European Legal Informatics Study Programme

MASTER'S THESIS (DOUBLE DEGREE):

COOKIES IN THE EUROPEAN DATA PROTECTION FRAMEWORK

By:

Riccardo Andrea Junior Varisco

Supervisor:

Dr. Marcelo Corrales, LL.M.

Date of submission: September 19th 2018

Deadline for submission: September 20th 2018

To Federico Faggin, creator of a marvellous future
To Sophie M., future creator of marvels

ACKNOWLEDGEMENTS

I would like to thank those who made this work possible: my parents, my Oslo Team: to Tugba A., to Esen Esener, to Benedikt F., to Raluca Stoica (especially for the help in finding a thesis’s supervisor) and to 余文洁.

I would also like to thank the Eulisp 2017-2018 and all the special people who have always helped me: Laura G. and Manuel B., Claudio G., Amedeo and Vanessa M., Davide P., Consul Federico R., Marces S. and Martin S. Fabio M.

TABLE OF CONTENTS

Contents

ACKNOWLEDGEMENTS....5
TABLE OF CONTENTS....7
LIST OF ABBREVIATIONS....9
INTRODUCTION....11
CHAPTER I: Technical Background....15
1.1 What is a HTTP Cookie?....15
1.2 Structure and technical implementation....16
1.3 Usage and risks....18
1.4 Cookies classifications....21
1.5 Flash cookies....22
1.5.1 Zombie cookies....23
1.5.3 Supercookies....23
1.6 Cookies as metadata source....23
CHAPTER II: Legal framework in Europe....25
2.1 Introduction to Cookies legal regime in Europe....25
2.2 E-Privacy Directive....26
2.3 E-Privacy Regulation....28
2.4 GDPR....31
2.4.1 GDPR Principles: Purpose limitation....32
2.4.2 GDPR Principles: Data Minimisation and Storage Limitation....34
2.4.3 GDPR Principles: Archiving....36
2.5 WP29 Opinions on Cookies....37
2.6 The possible futures....39
CHAPTER III: Case law and current issues....41
3.1 Cookies and Consent....41
3.1.2 Browser settings....43
3.1.3 Other systems....44
3.1.4 Is a well-informed consent possible?....45
3.2 GDPR rights and the zombie problem....46
CHAPTER IV: Cookies in the Big Data Era....49
4.1 Automated decision-making and profiling....49
4.2 Profiling....50
4.3 Behavioural Targeting and Tracking....52
4.4 Cookie Policies....53
4.4.1 Google and YouTube....53
4.4.2 Amazon....54
4.4.3 Facebook, WhatsApp and Instagram....55
4.4.4 Twitter....56
CONCLUSIONS....57
BIBLIOGRAPHY....59

LIST OF ABBREVIATIONS

CSRF	Cross-site request forgery
DNS	Domain Name System
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECJ	European Court of Justice
EDPB	European Data Protection Body
EPD	E-Privacy Directive
EPR	E-Privacy Regulation
EU	European Union
GDPR	General Data Protection Regulation
HTTP	HyperText Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocols
WP29	Article 29 Working Party
XSS	Cross-Site Scripting

INTRODUCTION

Rarely has a word caused an ambivalent mixture of feelings more than “cookies”.

At the same time, it refers to a pleasant culinary reward and one of the most annoying experiences for internet users: when one opens a website, a cookie banner is always present.

Years ago, a cookie banner was not something common. The banners started to appear massively only after 2009.

They can present themselves in different forms: it can merely reference a cookie policy to a user, it can ask for consent or it can even allow advanced setting for cookies, which has become more and more common after the entry into force of the General Data Protection Regulation (“GDPR”).

But what is the mystery behind those banners? What exactly is a cookie and why is it so important?

To understand what is at stake, I would suggest to the reader to do the following experiment as I did it.[1]

The aim is to check the average presence of cookies and, in order to achieve a better degree of impartiality, I used different techniques to count them.

Firstly I selected a famous website that automatically checks the number of cookies involved (http://www.cookie-checker.com).

Secondly, I simply check the cookies as indicated by my browser: Mozilla Firefox (tools>web developer>web console>storage folder), one ad-block and anti-tracker (AdNauseam) was running.

Last, I have Installed a new browser (namely: Chrome) and removed all the useless add-ons. I have installed two privacy add-ons (between many, I chose redmorph and ghostery) and one cookie analyser (EditThisCookie).

I have also cleaned the navigation history, emptied the cache memory and delete the cookies every time I changed web page.

The astonishing results are the follow:

[1] Experiment conducted on June 11th 2018, in Italy. Kali Linux was the operative system, Chrome was run via Wine.

Table 1: cookies used by commonly used website

Web Site / Technique	Cookies-Checker	Firefox	Chrome
Facebook	Unable	12 FPC; 0 TCP	9 FPC; 2 TCP
Google	2 FPC; 0 TPC	8 FPC; 0 TCP	4 FPC; 1 TCP
Amazon.com	7 FPC; 0 TPC	11 FPC; 0 TCP	7 FPC; 4 TCP
Linkedin	8 FPC; 0 TPC	14 FPC; 0 TCP	9 FPC; 3 TCP
Twitter	4 FPC; 0 TPC	9 FPC; 0 TCP	6 FPC; 3 TCP
YouTube	4 FPC; 0 TPC	12 FPC; 0 TCP	6 FPC; 6 TCP
Instagram	11 FPC; 0 TPC	10 FPC; 12 TCP	2 FPC; 2 TCP
The Guardian	8 FPC; 6 TPC	2 FPC; 0 TCP	2 FPC; 11 TCP
WSJ	27 FPC; 8 TPC	6 FPC; 0 TCP	7 FPC; 5 TCP
En.wikipedia	3 FPC; 0 TPC	3 FPC; 0 TCP	3 FPC; 2 TCP
Leibniz University	2 FPC; 0 TPC	1 FPC; 0 TCP	1 FPC; 1 TCP
University of Oslo	6 FPC; 0 TPC	1 FPC; 0 TCP	6 FPC; 0 TCP
PornHub	1 FPC; 1 TPC	9 FPC; 4 TCP	9 FPC; 9 TCP

Note: FPC: First Party Cookies, TPC: Third Party Cookies

Moreover, Redmorph reported that in twenty minutes spent for conducting this experiment, the browser has been followed by a total of 322 other trackers (web bugs, unique identifiers and so forth).[2]

Before commenting the results, it must be noted that the choice of browsers and operative system was not irrelevant: using others would arguably give different results.[3]

The Instagram results found an explanation in the fact that the twelve third party cookies belong to Facebook, which owns also Instagram, and was not accessible via cookie-checker. Last, as I do not owe an Instagram, a Twitter or a PornHub account, the count has been therefore reduced: I just accessed the web sites, further interactions would have surely created more cookies.

What it can be inferred by these data is that: an analytical site is probably unravelled as such and it gives a reassuring output.

An ordinary session has the most first party cookies, due to the log in and the continuous interactions, but the importance of an ad-blocker is fundamental: without the third party cookies would have probably be similar to the third column.

[2] A more detailed overview on browsers fingerprints: (Eckersley, 2010)

[3] For a technical analysis of how it has affected the privacy checker: (Schweighofer et al, 2017, pp. 185-188)

A completely new session generates less first party and more third party cookies. But, most important, my Internet Protocols (hereinafter: “IP”) was recognised as a European one and, therefore, they send different cookies along with the cookie banners.

This can be considered a prove of the fact that the so-called “internet” is neither a happy global village nor an uncharted far west. It is still bound to the germane territory, to a certain extent, and the impact of the European Union (hereinafter: “EU”) can be easily noticed. How it effects everyday internet life and how this happens from a legal point of view will be the central core of this work.

It will deal mostly with the current legislation (*de lege lata*), the ePrivacy Directive (hereinafter: “EPD”) but it will try to foresee the future development of the European legislation (*de lege ferenda*), namely the upcoming E-Privacy Regulation (hereinafter: “EPR”).

Furthermore, this work will deal directly with cookie policies of the most famous and commonly used web sites (Facebook, Google and Amazon), although this could be more bitten than expected.

CHAPTER I: Technical Background

The word "cookie" was chosen by computer scientist Lou Montulli[4], who had the idea of cookies in June 1994. He derived it from "magic cookie", which is the name of a data packet or a token sent unchanged by a program in Unix system.[5]

Originally they were known as "Netscape cookies" because they were invented and used by Netscape[6] – where Mr. Montulli was working at that time – in the Netscape Navigation Browser, which became available in September 1994. The purpose of cookies was to manage the stateless[7] Hypertext Transfer Protocol[8] (hereinafter: "HTTP").

1.1 What is a HTTP Cookie?

From a more general point of view, a cookie is just a small file stored inside a local browser directory by a web server.[9]

Technically, it is a system that allows a server to pass data and associated metadata to a user and it remain unchanged if the server is accessed again.[10]

When a server receives a HTTP request, it responds. The response contains three part: a request line, one or more headers and the response entity itself.[11]

A cookie can be included into the headers: it is created by the set-cookie function and sent in a set-cookie response header, which can contain different (arbitrary) information.

If the browser accepts a cookie, a small document[12] is saved in a directory, usually a browser directory. The amount of information and the content are established by the server.

[4] (Schwartz, 2001)

[5] (Catb.org, 2003)

[6] An automatic HTTP cookie management system (Yue, Xie and Wang, 2007).

[7] In computer science "stateless" means that each request message can be understood in isolation. In other words, there is no recorded continuity (Fielding, 2014).

[8] The HTTP is basically the foundation for the Web. Cookies are just an addition to it (Kristol, 2001, pp. 3-4)

[9] (Kristol, *supra* at 5)

[10] (Barth A., 2011, pp. 3-6)

[11] (Kristol, *supra* at 3)

[12] Some browsers, like Firefox, do not each cookie, but one single file, containing them all (AliceWyman – away et al, 2018).

Once a cookie is stored in a browser, it is shared to a server according to the same origin policy.[13] Such policy establish whether a HTTP request should contain a cookie, which must belong to the host according to the domain attribute or the Domain Name System (hereinafter: “DNS”) itself.

The opposite of a cookie is a session, which is stored in the server. Different to cookies, but sometimes similar in the aims, are plug-ins[14], server logs[15] and web beacons[16].

1.2 Structure and technical implementation

Cookies can be considered a typical example of a technical innovation that was developed before their standard was adopted.[17]

The current standard is defined by the Internet Engineering Task Force (hereinafter: “IETF”), which sets the *de facto* standard for internet[18], and it is the standard RFC_6265, which has replaced the obsolete RFC_2925.[19]

A cookie can be created in different programming languages – e.g. JavaScript, PHP and Phyton – and every language allows a different set of characters (alphanumerical and special) but some aspects remain the same.

In JavaScript, the creation of a cookie begins with the assignment of a name-value pair to a document.cookie object. For example, a cookie with name “cookie1” and value “examplecookie” would be:

document.cookie="cookie1=mycookie"[20]

Along with this basic pair, a cookie can carry different attributes: Comment (short description of the intended use of the cookie), CommentURL (it contains an URL to the comment), Domain (DNS domain or IP address for which the cookie is valid), Max-Age (maximum period after which the

[13] (Rabinovich, 2013, p. 1)

[14] A plug-in is a software component that adds a specific feature to an existing computer program (Mozilla Foundation, 2018)

[15] A server log is one (or more) file automatically created and maintained by a server. It contains a list of activities it performed (Garnica G., 2018, pp. 102-103).

[16] A web beacon is technique to track users that consists in embedding, for example, a small imagine (.gif or .png), in a HTML page. Whenever a user opens a page containing it such image is downloaded, without the user to be aware of it. One of the most famous beacon case was the Facebook Beacon that led to a ruling against it in 2010, see: *Lane v. Facebook Inc.* (Steeves V,, 2009, pp. 183-187)

[17] (Rabinovich, 2013, *ibid*.)

[18] (Kristol, *supra* at 8)

[19] Standard RFC 2965 was not the first IETF, which was RFC 2109. It should be noted that, standard RFC 2965 was never widely adopted.

[20] (Olsson, 2015, p. 51)

cookie must be discarded), Discard or Expiration Date[21] (when the cookie should expire), Path (subset of URLs on qualifying hosts for which the cookie is valid), Port (list of TCP ports on qualifying hosts for which the cookie is valid), SameSite (which prevents the browser from sending a cookie along with cross-site requests) and Secure (if present, the cookie may be transported only over a secure channel: e.g. SSL-protected, HTTPS).[22][23]

In PHP, the set-cookie, which must be called to create a cookie, must have three mandatory parameters: name, value and expiration date. For example:

setcookie("example", date("H:i:s"), time() + 60*60);[24]

The name is “example”, the value is the date function and the expiration date, measured in seconds, is usually set relative to the current time in seconds retrieved through the time function: in this example, the cookie has a Max-Age, which is set to expire after one hour. The aforementioned attributes can be added too. Moreover, an interesting attribute that PHP (or Python) can add is HttpOnly: if it is present, the cookie cannot be accessed by a client-side script (JavaScript).

In Python, a more elaborated example of a set-cookie could be:

Set-Cookie: session=12; expires=Wed, 13-Jun-2018 00:01:00; path=/; domain=exampleserver.com

The paid name-value is “session=12”. In this line the expiration date and the domain have been added.

Independently from the languages used, a cookie can be deleted manually, by creating the same cookie again with an old expiration date. In such case, it is removed when the browser is closed.

Basically a cookie must always have a name=value structure. However, these three examples show that examining a cookie’s value does not necessary reveal what the cookie purpose or what the value represents.

Once is created and stored in the browser, the server relies that the cookie will return the next time the server receives a request. In this way, it is possible to track a user: it is not relevant whether the IP changes, as long as the cookie remains, a user would be recognised.

[21] Although the practical result would be the same, the Max-Age is different from Expiration Date. Besides the technical differences, one has the expiration based on seconds in the future and the other a date, the default expiration of a cookie is the session, while there is not default Max-Age. However, Internet Explore is not supporting Max-Age: https://mrcoles.com/blog/cookies-max-age-vs-expires/

[22] Another attribute was “version”, which was a decimal integer that identified to which version of the state management specification the cookie conforms, but it has been rendered obsoleted by RFC 2965.

[23] (Rabinovich, *supra* at 2)

[24] (Olsson, 2016, p. 103)

Last, an important element that arises from the technical analysis is that cookies are a communication – bulk communication to be specific – between machines, without human intervention.[25]

1.3 Usage and risks

Cookies have many different purposes. Most of them are *prima facie* legitimate.

One of the most often cited reason is authentication and security.[26] A cookie that contains an identifier[27] can help a server to identify a device and, therefore, it makes the authentication more secure:[28] if there are two servers involved – one for the identification process and one where the passwords are stored – such cookie can relate the two, giving a strong level of security. Cookies can also allow a recovery of an account, if the account has been violated by a third party. They can be deployed to fight spam and phishing. They also allow to remember a user, without the inconvenience of logging off, or to respect its internal policy or laws.[29]

Another common reason is preferences. Cookies allow to save and remember there preferences, settings or themes: such as browser data (software, version and so on) local region and language or personal settings (size, font and so forth). This functions is extremely important to allow a personal experience of a website: weather news, time or even traffic[30] news. However this are not fundamentals data and a site can work even without them (but it results in a less performing experience).

In order to work properly and deliver a service a web site can deploy cookie to help the actual processing. They can help to route the data traffic through different servers or other specific functions: the “lbcs” cookie (Google owned) that allow Google Docs to open many Docs in one browser or the “sb” cookie (Facebook) which is important for friends suggestion.

[25] (Carmi, 2017, pp. 289-307)

[26] Basically every cookie policy states that cookies are used for security reasons: Google cookie policy, Facebook cookie policy, Amazon cookie policy, Twitter cookie policy and so forth.

[27] They permit a good identification of a user. This is a relevant reason for their usage: it is easier to use a cookie to identify a user, than, for example, the IP, which is unreliable. (Kristol, *supra* at 6)

[28] However, this cannot help against the theft of hardware. It can also be a quite annoying experience for a user that needs to change equipment, especially if the the cookie contains geolocalion data and such necessity happens in a country where the user does not live habitually.

[29] In the Facebook cookie policy is written that cookies prevents minors to create an account (the effectiveness of this should be further evaluated).

[30] This is for example the Google cookie policy.

Another reason, very important for business purposes, is to collect session state data, which are the data generated by the interaction of users with a website. The range of possibilities is very wide: a track of the interaction with goods on Amazon, the last video watched on Youtube or just an analysis of the interplay with the advertising.[31] Even in this case, it is possible to disable or delete such cookies.

An apparently innocent reason is the statistical analysis of a web site: how a user engages with the website or as an aid for advertising cookies. Unfortunately, due to the *de facto* dominant position of Google, it is often synonym of Google's analytics cookies.[32][33] Google's main cookie for this is "__ga" and it collects data in an anonymous way.[34]

Last, the most (in)famous reason for using cookies: advertising.

When on April 10th 2018 Marc Zuckerberg was called to testify before Congress for the Cambridge Analytica case and he was asked by senator Hatch about the business model of Facebook. The Facebook President replied "Senator, we run ads" and then he smirked.[35]

That phrase could be considered as a summary of the business model of those websites that are not engaged in e-commerce. It describes perfectly social networks and it subtly implies that they are a database of tastes and trends, on those they rely for their market value.[36] How do they achieve that? Among others, cookies.

It should be obvious that this is not a one-cookie job. It is not just the "fr" cookie (Facebook), the pair "IDE"/"ANID"[37] cookie (Google, for non-Google advertising) or "ad-id"/"ad-pref-session" (Amazon), but a synergy of these cookies with other cookies, used for the purposes listed above. These cookies have a wide range of data: tracking users (if a user visit a website, these cookies allow to follow the user through the web showing ads from that site), users' activities (e.g. how many times an ad has been clicked), statistical (how many times an ad is visualised), variety (they prevent to show always the same ad on one or more devices) and more.[38]

[31] For a critical approach on how these data can be used for personalising the prices: (Zuiderveen Borgesius and Poort, 2017, pp. 1-3)

[32] In the experiment performed in the introduction, all the third party cookies were related to this category.

[33] (Cookielaw.org, 2018)

[34] For a brief explanation about how to de-anonymise anonymous data sets see: (O'Neil, 2016, pp. 68-83).

[35] (Holman, 2018)

[36] (Turban, 2017, pp. 14-16)

[37] "IDE" is stored in browsers under the domain doubleclick.net and "ANID"is stored in google.com. In 2018, Google has re-branded DoubleClick to Google Marketing Platform, however the Google cookie policy keeps referencing to doubleclick.net.

[38] For example, Facebook has cookies for analysing the likes and shares of a product.

Along with these (mostly) lawful purposes, there are many risks. Focusing on the technical – legal and economic risks will be covered in the following chapters – cookies pose a relevant security treat.

The problem of cookies and privacy and security is actually old. The history of the RFCs standards shows that during the first two standardisation, the security and privacy issue was taken into account and delayed the standardisation process: there was a tension between the two working group (the Internet Engineering Steering Group and the HTTP Working Group) about privacy safeguards (stricter for the steering group, weaker for the other).[39]

A general and known problem is that, even if a browser saves only the cookies received by a server, it can happen that a browser could visit many servers on a user's behalf and the user would have no knowledge of it.

Moreover the attribute "secure" does not necessary means that a cookie is safe: if the machine has been compromise, using a HTTPS would not improve the security. Moreover there is no defence from the human element (e.g. social engineering)

Other vulnerabilities involve Cross-Site Scripting[40] (commonly known as "XSS") and session hijacking.[41] As cookies authenticate a user, these attacks can lead to an enormous damage: not just the data in it are stolen, but the cookie itself on which a server relies.[42]

Last, the most relevant attack that should be mentioned is the cross-site request forgery (hereinafter: "CSRF").

If a user has paid something or accessed a bank account and the related cookies have not been deleted, that user is exposed to a CSRF attack. It is an attack that exploit a website where unauthorized commands are transmitted from a user that the web application trusts.[43] For example, image tags, hidden forms and JavaScript XMLHttpRequestsn can be included in a website and their purposes it to steal payment or bank data. In this situation, cookies are exploited. Standards and practices have been developed[44] to avoid this attack, however, in general, for a user, it is good practice to regularly delete cookies, especially every time a security breach occurs.

[39] (Kristol, *supra* at 13)

[40] It is an attack in which malevolent script is injected in a website (Seyyar, 2017, pp. 28-29),

[41] For a technical and complete paper: (Dabrowski et al., 2016)

[42] This was one of the reasons for the introduction of attribute "HttpOnly": it can help to mitigate this attacks by preventing access to cookie, exploiting vulnerabilities of JavaScript (Aycock, 2011, pp. 116-117)

[43] (Ristic, 2005, p. 280).

[44] For example, including a synchronizer token pattern in the page HTML or, for what concerns cookies, improving the same origin policy and setting short expiration date (Liu, Kovacs and Gouda, 2010, pp. 1724-1728).

1.4 Cookies classifications

Cookies as tools are classified in a unitary way: a cookie is a cookie. However, they can be divided for technical or legal reasons.

An important technical subdivision is by the expiration: there can be session cookies and persistent cookies. The first kind of cookie is erased when the session ends and the other one remains across multiple sessions.[45] Persistent cookies are commonly used for password memorisation (Chen and Sivakumar, 2005, p. 1528)

Another relevant distinction is the categorisation by the sender: if a cookies is set by the main page is a first party cookie, while if it is referencing other resources across the web is a third party cookie.[46]

Concretely, it means that visiting www.socialnetwork.com, which contains ads from an undertaking called Evil Corp, will entail a download of a cookie belonging to ad.evilcorp.com. If a user then visit another website, www.shop.com, which also contains ads from ad.evilcorp.com, a new cookies, belonging to the Evil Corp., is downloaded. Eventually, both of these cookies will be sent to the advertiser when loading their advertisements or visiting their website. The advertiser can then use these cookies to build up a browsing history of the user across all the websites that have ads from this advertiser.[47]

Last, the UK International Chamber of Commerce ("ICC") proposed[48] a classification based on their purposes: there are Strictly Necessary Cookies, Performance Cookies, Functionality Cookies and Targeting or Advertising Cookies.[49]

Strictly Necessary Cookies means that those cookies are essential in order to enable the website and its features (e.g. accessing secure areas or shopping baskets).

Performance Cookies are cookies that collect information, without identification, about how visitors use a website (pages most visited, error messages) and the data (aggregated and anonymous) are only used to improve how a website works.

[45] (European Commission, 2017)

[46] (European Commission, 2017)

[47] (Backes M. et al., 2012, pp. 260-263)

[48] (ICC UK, 2012)

[49] For a further legal analysis: (Bond, 2012, pp. 220-223)

Functionality Cookies. These cookies allow the website to remember choices (user name, language, region and so forth) and provide enhanced, more personal features. Anonymisation can be implemented or not.

Targeting/Advertising Cookies are cookies used to deliver target and personal adverts. They are usually placed by advertising networks with the website operator's permission. They remember that a user has visited a website and this information is shared with other organisations such as advertisers. Quite often targeting or advertising cookies will be linked to site functionality provided by the other organisation.[50]

Although this classification is used[51], it is mostly useful for legal reason.[52] It is relevant as the Article 29 Working Party[53] (hereinafter: "WP29") wrote an opinion that explained how these categories relate to consent (see 2.5 WP29 Opinions on Cookies).

1.5 Flash cookies

Another category, completely different from HTTP Cookies, is Flash Cookies.[54]

Flash cookies, technically called "local shared objects," are files used by Adobe Flash developers to store data on users' computers via Adobe's multimedia Flash plug-in.

Their primary purpose is not to track users, but to provide Flash applications with options to save data to the local system: for example, for running Glash games. They are often used as they can hold up to 100kb rather than just the 4kb held by HTTP cookies.[55]

Due to their flexible technical nature, these cookies can be programmed in a way whose legality is doubtful.

[50] (ICC UK, *supra* at 9)

[51] For example, it is mentioned in the cookies policy of ICANN and it has partially been accepted by WP29 Opinion 04/2012.

[52] It could be hard, from a technical point of view, distinguish what is strictly necessary and what is related to the performance or the functionality of a website.

[53] It should be noted that the WP29 has ceased to exist. Its functions are now included in those of the European Data Protection Body (hereinafter: "EDPB").

[54] (McDonald and Cranor, 2012, pp. 640-642)

[55] (Sipior, Ward and Mendoza, 2011, p. 3)

1.5.1 Zombie cookies

Zombie cookies or evercookies are those cookies that “respawn”. They recreate themselves automatically after being deleted.[56] This is possible because this cookie is stored in multiple locations: Flash Local shared object, HTML5 Web storage and other client-side and even server-side locations.[57] If a cookie is deleted from any of the storage mechanisms, a copy aggressively re-creates it in each mechanism (as long as one is still intact).

Moreover if the Flash LSO, Silverlight or Java mechanism is available, Evercookie can propagate cookies between different browsers on the same client machine.[58]

1.5.3 Supercookies

A ordinary cookie as a specific domain name (aforementioned: exampleserver.com), while so-called supercookies has just a top-level domain (.com) or a public suffix (.com.de[59]), allowing a cookie not created by exampleserver.com to be sent to it, due to the domain .com and therefore rising security issue: it can infect the server with malicious code. There cookies are mostly flash cookies, but they can be also HTTP.[60] Moreover they can track user in a very intrusive way, using machine identifier or Etag.[61]

1.6 Cookies as metadata source

Cookies collect data, both personal and non-personal[62] data. But they can also be used to collect metadata.

[56] (Angwin and Tigas, 2015)

[57] (Sörensen, 2013, pp. 321-322)

[58] As described on the blog of the creator: (Kamkar, 2018)

[59] For a complete list see: (Publicsuffix.org, 2018)

[60] (ENISA, 2012, p. 11; Schoen, 2009)

[61] An ETag is an opaque identifier assigned by a web server to a specific version of a resource found at a URL (Hoofnagle et al., 2012, pp. 281-282).

[62] The *vexata quaestio* of non-personal data will not be covered by this thesis. It is simply assumed that cookies can be used for collecting them. It must be noted that a Brobdingnagian amount of data traded and shared are non-personal. However there is currently no legal tool in EU, just a proposal: Proposal 2017/0228.

Metadata are, according to a common definition “data that provide data about other data”[63][64] (e.g. in respect of a photo, metadata are data about colours, resolutions, time and place of creation, size and so forth).

Metadata can be divided into three main categories: descriptive (identify and discover), structural (how information is put together) and administrative (manage information and show data about it).[65]

Considering this thesis as a data, descriptive metadata would be title, author or abstract, structural page order to chapters and administrative the data that the university will implement to store and share this work.

They have many purposes. They can organise efficiently electronic resources, especially websites. They facilitate interoperability and integrating resources (especially, it counters typical data entropy and degradation). They can allow the so-called internet of the things to work more effectively. They can ameliorate digital identification. Last, they can be used to analyse huge amount of data: the espionage conducted by the United States is, among other techniques, based on metadata analysis (also Google, Twitter and Facebook, in analysis contents and emails, use metadata analysis).[66]

It is easily understandable how cookies can transmit all the information necessary to create ample datasets in which data and metadata are mixed.

[63] (Pomerantz, 2015, pp. 19)

[64] For a critical approach to this definition: (Pomerantz, *supra* at 20-22).

[65] (Pomerantz, *supra* at 65-116).

[66] (Pomerantz, *supra* at 117-152).

CHAPTER II: Legal framework in Europe

From a legal point of view, cookies is a issue that was addressed relatively late: the use started in mid-90s, but most jurisdiction preferred to ignore it.

Considering what is at the stake and the internationality of internet, it would have been a more appropriate to have the problem solved out in the context of international law. But as there is not international treaty on internet, privacy or data protection – although there are important articles in the context of the human rights field[67] and Convention 108[68] of Council of Europe – there is no global rule about cookie.

The EU has reacted slowly: the first effective measure was introduced only in 2009, almost fifteen years after the introduction.

2.1 Introduction to Cookies legal regime in Europe

The current European legislative framework for data protection, which descends from the treaties[69], can be described as comprehensive[70], but it must be considered a "work in progress", that will change years after years: new acts, new interpretations of them made by the European Court of Justice (hereinafter: "ECJ") and even national laws (even if they have a limited impact).

Currently, the backbone of the European Data Protection Law (and not just Europe[71]) is the GDPR, approved on April 27th 2016, in force since May 25th 2018 and replacing the data protection directive 95/46/EC.[72]

[67] Art. 12 of the Universal Declaration of Human Rights, art. 17 of the International Covenant on Civil and Political Rights and art. 8 of the European Court of Human Rights.

[68] The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was the first international tool that deals with data protection and international data flow. Interestingly is a treaty open for accession of non-member States, currently the most important non-member State that has ratified it is Mexico (others include: Senegal, Tunisia and Uruguay). For the complete list with dates: (Council of Europe, 2018)

[69] The main provision about privacy can be found in the Charter of Fundamental Rights in art. 7 and, interestingly, art. 8, which is an explicit provision for data protection. Moreover art. 16 of the Treaty on Functioning of the European Union recognises data protection as fundamental right in itself.

[70] In contrast to the American one, which is sector specific, or the self-regulatory approach of Japan (Densmore, 2013, p. 19)

[71] Among others, the recent Brazilian Data Protection Act, the proposed Indian Data Protection Bill, the California Data Protection Act have been inspired or have copied from the GDPR.

[72] It must be noted that the GDPR applies only to natural living persons, not to deceased persons (recital 27) – however, in Italy, rules have been established: art. 9 of Italian Privacy Code allows heirs or whoever holds a legitimate interest to enforce GDPR rights – and not to legal entities (although countries can expand the protection even to them, like Austria or, outside the EU, Norway have done).

Revolving around the GDPR, there are other regulations and directives: the EPD[73], which is a *lex specialis* to the GDPR, the Regulation 45/2001/EC on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, the Directive 2016/680[74] and the Passenger Name Record Directive, officially known as Directive 2016/681.[75]

Cookies were generally covered by the Data Protection Directive, but entered specifically into the EU legislation thanks to the EPD.

2.2 E-Privacy Directive

The EPD is a sectoral directive focused on telecommunication. It repealed the Directive 97/66/EC (the Telecommunications Privacy Directive) and it was intended to complement the Data Protection Directive.[76]

The scope is to protect the legitimate interests of users and subscribers, who can be natural or legal person, in the context of "electronic communications services", but the definition of them was not in the EPD. It can be found in the framework directive (2002/21/EC) and it states "a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks". It has been interpreted[77] to apply only to telecommunication operators and not to over-the-top services (web services, mobile apps and so forth). Many issues depend on how a Member State has transposed the EPR[78], but for what concerns cookies, this is irrelevant, because article 5(3) is a general norm that applies to any services, including e-commerce, as clarified by WP29.[79]

The directive was amended in 2009 and, among other things, like new rules for data breach notification, it introduced rules for cookies. The first formulation of article 5(3) was:

[73] Directive 2002/58/EC on Privacy and Electronic Communication.

[74] On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

[75] Other rules can be found in different kind of documents, like those related to competition in the internal market or even the directive 2016/65/EU, on markets in financial instruments (so-called "MiFID II"), in article 78.

[76] The developers of cookie-checkers.com, for a critical approach to the directive: (Trevisan, et al, 2017)

[77] (Gutwirth, Leenes and De Hert, 2016, pp. 214-215)

[78] For example, regarding the British transposition, it applies to all devices, not just those that process personal data. While Italian Authority (*Garante pre la Protezione dei Dati Personali*) strictly narrowed it to personal data (in Italian): (Garante della Privacy, 2014)

[79] WP29, Opinion 1/2008, p. 12

> “Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.”.

After 2009:

> “Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service”.

The phrase “the storing of information, or the gaining of access to information already stored, in the terminal equipment” is actually broader then just cookies. It also refers to a series of software, often malicious, that can spy and track users (spyware, eTags or hidden identifiers[80]). But, as recital 25 makes clear, cookies, when legitimate, are a tool that fulfils important purposes (e.g. verification of a transaction).

The new rule introduced the concept of (prior) informed consent for the storage of cookies. As imaginable, exceptions were provided too: cookies are exempted from consent when they are used for the sole purpose of carrying out the transmission of a communication and when they are Strictly necessary in order for the provider of an information society service explicitly required by the user to provide that service (e.g. authentication cookies).

A requirement that has not changed from one version to the new one is the obligation to inform and obtain consent.[81] The only changing was about the offering: before 2009 the possibility to refuse should have been allowed, after it is required an affirmative consent to store the cookies. Different mechanisms have been proposed for reaching this goal: browser settings and opt-out[82]. The problems related to these, as well as consent, will be discussed in the next chapter.

[80] Recital 24 of EPD.

[81] (Kosta, 2013, pp. 381-386)

[82] Opt-out means that a user has the right to object the use of cookies, while opt-in means that a user explicitly chooses to use them.

2.3 E-Privacy Regulation

The EPD ended in a fragmented legislation across the EU[83], the European Commission is seeking[84] to a strong level of harmonisation via regulation: the EPR.

The EPR will adjust the data protection rules for electronic communication services to GDPR[85], however it is not clear to what extent: a furious lobbying is ongoing on this proposal.[86] The current problems are related to the widening of the scope (the attempt to include the over-the-top), the rules for metadata, stricter rules for cookies and tracking technology, opt-in rules for direct marketing, harsh rule for spam ("unsolicited calling"), browser settings as manifestation of consent and other relevant issue (e.g. the shift from telco regulator to data protection authorities, the same sanctions of GDPR). It is not easy to foresee what will survive and what will be ceased under the fire of lobbying.

Focusing of the cookies issue, the scope of the EPR is to have simple and clear rules for cookies. However the current drafts tend to differ.

In the January 2017 draft the main articles[87] are 8, 9 and 10, which are integrated by recital 20, 21, 22, 23 and 24.

The rule is set as a general prohibition going along with many exceptions, namely article 8 contains two main prohibitions, art. 8(1) and 8(2), and one recommendation, art. 8(3) and 8(4). Regarding the "use of processing and storage capabilities" is permitted only for the "sole purpose of carrying out the transmission", "consent", "providing an information society service requested by the end-user" or "web audience measuring". These exceptions allow companies to use strict necessary, performance and functionality cookie. For any other kind (especially targeting) consent is necessary.

Regarding the "collection of information emitted" – the information transmitted by a cookie – it is allowed only when "it is done exclusively in order to, for the time necessary for, and for the purpose

[83] For an overview: (DLA Piper, 2016)

[84] Currently, 22nd July 2018, the EPR is still a work in progress. The Commission's desire to approve it simultaneously with the entry into force of the GDPR failed. It is also very unlike that it will be approved this year and dubiously it will be approved in 2019.

[85] For a critical article about the interaction of the two Regulations: (Cormack, 2017)

[86] (Meyer, 2017), but for a critical approach (Naranjo, 2017)

[87] (European Commission Proposal, 2017)

of establishing a connection" or "a clear and prominent notice is displayed". Moreover, the collection must follow the appropriate safeguards according to article 32 GDPR. Last, the article recommends to integrate the aforementioned notice with standardised icons, which can be provided by the European Commission.

Moreover, article 9 sets forth the consent under the light of GDPR, but at paragraphs (2) and (3) introduces some interesting rules: first, it lays down that consent can be provided by the browser settings. This, as explained by recital 23, would prevent users to be "overloaded with requests to provide consent". In this way, the choice made by a user regarding its setting must be considered binding on third parties. The idea behind, as explained by recital 23 (referencing article 25 of GDPR), is that browser settings should apply those principle of privacy by default and by design in order to avoid the "accept all cookies" standard used by many browsers. Last, it creates a special regime for withdraw, giving a six months interval to remind the possibility of withdraw. Last, article 10 strengthens the possibilities to prevent third parties from storing information or processing information already stores, like, but not limited to, HTTP and Flash cookies, on the end-user equipment. It also states that a user must be informed, in an effective way, of all the options and his or her consent is required by a web site or a mobile app. These rules have been strongly criticised[88]. The EU data, gained via survey, show that when a user can choose, it would refuse cookies.[89]

In the March 2018 draft[90] left the rules about cookies unchanged. But in the April 2018 draft[91] the rules changed significantly.

A new exception was added to article 8(1): necessity to security update.[92] But article 8(2) was changed in a more extensive way. The collection of emitted information is allowed to maintain the connection, if the consent has been given and to conduct anonymous and necessary statistical counting.
Article 9 was deleted and article 10 was strengthened: not just to prevent third parties, but "any other parties than the end-user".

These new rules can be reckoned more friendly to telc, which can rely on more exceptions. In order to mediate the different instances, in the May 2018 draft[93], written under the Bulgarian Presidency,

[88] (Fazlioglu, 2018)
[89] (Flash Eurobarometer 433, 2016)
[90] (Council Proposal March, 2018)
[91] (Council Proposal April, 2018)
[92] The condition for this new exception is that: security updates are necessary, do not change privacy settings, the end-user is informed and the possibility to postpone such update is given.
[93] (Council Proposal May, 2018)

other radical changes were introduced. Article 9 was reintroduced, as number 4, and it added a relevant new rules: consent of a legal person (through its representative, according to the national law). This new provision went even beyond the rules of GDPR. It was a way to protect not only consumer, but also small and medium enterprise, in their relationship with IT corporations. It reaffirmed the browser settings as a system to express consent, but it expanded the six months interval to twelve.

However, a new exception was added to article 8(1): "maintain or restore the security of information society services, prevent fraud or detect technical faults for the duration necessary for that purpose".

Article 10 remained substantially unchanged.

This version obtained a fair balancing between the previous amendments and the users protection.

Last in the July 2018 draft[94], conducted by Working Party on Telecommunications and Information Society, article 4 and 8 remained unchanged, but article 10 was deleted. As stated in the document, the deletion occurred because that articled raised concerns "with regard to the burden for browsers and apps, the competition aspect, the link to fines for non-compliance but also the impact on end-users and the ability of this provision to address e.g. the issue of consent fatigue". It is interesting to point out how recital 20 was implemented in this draft. Before July, the decision around the so-called "cookie wall" was negative. Cookie wall means that consent to cookies should not be a "wall" that stops users to access a website, because it is "disproportionate".[95] However, in the draft it has been added to recital 20 that such wall is not disproportionate, in the context of website content provided without direct monetary payment, if a end-user is able to "choose between an offer that includes consenting to the use of cookies for additional purposes and an equivalent offer by the same provider that does not involve consenting to data use for additional purposes". This last draft was criticised[96], however the Presidency (Austria) intends to discuss it with the delegations.[97]

What would be the future of the EPR? It is hard to foresee.

Regarding cookies, it is considerably possible that the rules analysed proposed till now will not survive.

In one and a half year the number of the exceptions has significantly increased. The problem with

[94] (Council Proposal July, 2018)

[95] It should be noted that the EDPB backed the ban on cookie wall as contrary to GDPR: (EDPB Statement, 2018)

[96] (IT-Pol, 2018)

[97] It should be noted that, as stated, the EPR is not a priority fort the Austrian Presidency: (Meyer, 2018)

the attitude is that it does not find a concrete correspondence to what is written in recital 20 (or 21, till May 2018 draft), which aims to allow only those cookies that realise a minimum intrusion into a user's privacy. If the starting point was to obtain simple and clear rules for the whole Union, now there are many complicated exceptions.

This is not just a bad example of legal writing but softening the main rules and excessively relying on the consent could weaken another relevant aspect of EPR: sanctions. One of the its strengths should be article 23(2), (3) and (5), which set forth the same sanctions of the GDPR: ten and twenty millions of Euro (natural persons and public authorities) or 2% and 4% of total annual worldwide turnover (legal persons).

For what concerns cookies, article 8 and 10, the layer chosen is the lower: ten millions and 2%. However, the powers of the Authority are the same of those in the GDPR, to which it refers. This is supposed to lead to an peculiar situation: if it orders the stop of a processing, the penalties for not complying with this order is the hard layer. But if the EPR ends full of complicated exemptions, such sanctions would hardly be imposed.

For these reasons, the EPR should remain a relevant part of the European privacy debate. Because the only possibility for users to have their rights guaranteed is to exercise a strong moral suasion or to allow consumers' organisations to conduct a counter lobbying action.

2.4 GDPR

Outside the sectoral legislation, cookies are subjected to the data protection rules of GDPR, as long as they are able to identify a natural person. This interpretations can be derived by both the ECJ case law and from recital 30[98], which merely describes the technology that can be implemented to identify a natural person. Other than this, contrary to the EPD, the GDPR has no article that deals directly with cookies.

[98] "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them".

However, doctrine has elaborated that a cookies, when is installed into the browser, is covered by the GDPR[99], but, as affirmed by WP29, the rights of GDPR are without prejudice of the technology involved, as long as personal data are personal.[100]

This means that cookies are limited by the principles contained in article 5 and by the rights provided from article 15 to 22, among all the other requirements, e.g. the necessity of a Data Protection Impact Assessment (hereinafter: "DPIA"), that can be conducted by a Data Protection Officer (hereinafter: "DPO"), if, for example, a new kind of cookie is developed.

Such principles requires further considerations.

2.4.1 GDPR Principles: Purpose limitation

The principle of purpose limitation, as defined by the most updated version, article 5(1)(b), consists of three elements: first it sets forth that the data collected should be processed for a "specified, explicit and legitimate purpose". This entails that a controller must establish and reveal the purpose for which the data would be processed. Once it has been defined, it limits the operations of the controller, as, the second element states that data should not be further processed in "a manner that is incompatible with those purposes". Last, a specific derogation, which must meet the provisions of article 89(1) of the GDPR, is established regarding further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

The principle itself is not a novelty introduced by the GDPR: it can be traced in the Convention 108[101] and in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[102]. These two documents had an impact in developing the data protection framework in which the directive was elaborated and, later, the GDPR.[103] In it, the principle was transplanted essentially identical[104], but the third element has been expanded.

[99] *Inter alia*: (Voigt and von dem Bussche, 2017, p. 11; Hijmans, 2016, p. 497)

[100] Opinion 02/2012, p 2.

[101] Convention 108, article 5(b).

[102] OSCE Guideline, identical text in both versions (1980 and 2013), par. 9.

[103] Article 6(1)(b) of Directive 95/46/EC.

[104] The change of wording from "processed in a way incompatible" to "in a manner that is incompatible" does not entail a practical difference as "manner" and "way" are considered synonyms.

In relation to cookies, purpose limitation could be highly problematic. While strictly necessary cookies, by definition, do not pose any problem, the line tends to blur in relational to performance and functionality cookies.

The problem becomes more clear when the compatibility test applies. The meaning of it is specified by recital 50. That recital was strongly influenced by the Opinion 03/2013 on Purpose Limitation of WP29. The Opinion – largely based on the practices of Member States – explained in detail the provision of the directive and helped to construe the issue. As the WP29 pointed out, the Purpose Limitation should be assessed in a substantial way (and not in a purely formal one), in order to dispose of a certain degree of flexibility and sensibleness.[105] Furthermore, the WP29 elaborated four main key-factors, which can be found also in recital 50, for a substantial compatibility assessment: (a) the substantial relationship between the purposes for which the data have been collected and the purposes of further processing; (b) the context in which the data have been collected and the reasonable expectations of the data subjects as to their further use; (c) the nature of the data and the impact of the further processing on the data subjects; and (d) the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects. The practical impact of these criteria is relevant: if an assessment based on them produces a compatibility with the original purpose, no other legal basis is required for a controller. Otherwise, a controller should try to achieve one of the legal basis of article 6 of the GDPR, like a separate consent for further processing (which must be obtained before the processing based on the new purpose starts).[106]

Concretely, the example about preference cookies shows the problem: while it is reasonable to deploy those cookies to establish the language or the currency – which is a compatible processing – a further analysis of them to provide optimised traffic information could be problematic: depending on how accurately the position or the GPS data are elaborate, it could lead to an incompatibility with the original purpose.

More unclear would be if the cookies are processed or shared with others: for example, the compatibility of cookies used by Facebook, collected by Whatsapp, to suggest new friends should

[105] Opinion 3/2013, p. 21-22.

[106] Otherwise it would be a violation of a substantial norm, article 6, for lacking of a legal basis and, therefore, the applicable sanction would be in the highest layer: up to 10 millions or 4% of the total worldwide annual turnover of the preceding financial year: article 83(5).

be careful considered[107] and even more carefully considered if those data are shared with Linkedin, which is one of Facebook's partner.[108]

But if Facebook starts to process cookies to help, for example, lonely and people with suicidal tendencies to find friends and comfort? This is a typical grey zone of the purpose limitation that have led some authors[109] to declare that the assessment should be focused more on the interests than the original purpose, evaluating also the safeguards deployed.[110] The WP29 has tried to promote consent as the best solution to the purpose problem. However, as it will discussed in the next chapter, it is a fragile solution.

In a situation where data are dynamically and abundantly collected by cookies long before it is understood what the use could be, it is difficult to establish the final purpose in the first place.

2.4.2 GDPR Principles: Data Minimisation and Storage Limitation

Connected to purpose limitation, there are 5(1)(c) and 5(1)(e), which are the principle of data minimisation and the principle of storage limitation.

The first principle lays down that data should be stored and processed only if "directly relevant and necessary to accomplish a specified purpose […] data controllers should collect only the personal data they really need".[111]

The second one establishes that data, which allow identification of a subject, can be kept only as long as it is necessary. Once again, the derogation for archiving should be in accordance with article 89(1).

Complying with this principle entails not only to verify whether data retention policy of every relevant Member State, but also, if there is none, the adoption of an internal data retention policy.[112]

Cookies could be considered the archenemy of these two principles.

[107] Even if a Facebook account fakes its data, the statistical analysis of friends could reveal the information that a subject wanted to hide. After all, if a user has many friends from one city and interacts mainly with them, it has probably a real link or connection with it.

[108] Facebook cookie policy

[109] *Inter alia,* (Moerel and Prins, 2015)

[110] In this example, if Facebook's software wrongly considered a sad subject as suicidal, this could lead to important consequences to the subject's life, especially if the information is shared in the context of the subject's working life or family. GDPR provided article 22 for this kind of situation, but, as it will discuss, it is not clear if it works.

[111] Such definition is contained in (Glossary of the EDPS, 2018).

[112] It has been pointed out that this aspect has not been completely addressed and a guideline from the EDPB is expected.

The amount of data (personal and non personal) and metadata that a cookie can transmit is nor always easy to evaluate if it is really "relevant and necessary". Moreover the expiration of cookies is sometimes well set – Facebook implements a policy that ranges from thirty minutes ("asksb" cookie) to five years ("oo" cookie) – but often not: the "session-id" cookie, Amazon, lasts almost eighteen years and the "bs" cookie[113], PornHub, has an expiration date of almost sixty years, which is clearly in violation of what is "long as it is necessary", especially if the context and the purpose is evaluated.[114]

Unfortunately, anonymisation could not become an important springboard to accomplish, among other purposes, a data minimisation assessment for cookies[115]: some cookies can collect data on an anonymous way, it would be ludicrous to demand, for example, anonymous authorisation cookies. In this context, the most appropriate safeguard is most likely pseudonymisation[116][117] as would also allow undertakings to rely on further processing. However, if this could be burdensome for small business that wants to use cookies, which, on the contrary, are affordable.

However, data minimisation should try to achieve the avoidance of an unnecessary amount of data[118] in relation to the purpose, if it is possible to attain such purpose by excluding certain data from the processing.[119] This is once again an expression of the principle of privacy by design and by default and it could be a solution for some cases of usage of third parties and tracking cookies that rely on crossing of data set: a cookie owned by a cloths shop is even more valuable if can be integrated by data from, for example, a travel fare aggregator web site, but it is not relevant for the shop to know the exact destination, just generic data: if it must advertise a swimsuit or a winter coat. Even so, it should be remembered that it is often possible to infer sensitive information about

[113] It saves IP address, browser type and version, time zone setting and location, operating system and platform.

[114] WP29 in the Cookie Sweep Combined Analysis Report stated that: "Cookies with an expiry set to 31/12/9999 23:59 (the maximum possible value) could be regarded as not having a reasoned retention schedule defined […] the average duration was between 1 and 2 years. This could be a useful starting point for a discussion regarding an acceptable maximum duration, although the purpose of the cookie will also need to be taken into account."

[115] A consequence of anonymous of a data set is that, once it has been deprived of its unique identifiers, the resulting data would fall outside the GDPR scope.

[116] As defined by article 4(5): "'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;"

[117] According to GDPR: article 6(4), pseudonymisation is a factor that controllers should consider when determining compatibility of purpose for further processing; article 32(1), pseudonymisation may assist controllers in meeting security requirements; and Article 25(1), pseudonymisation an example of a measure that may satisfy requirements for privacy by design.

[118] This, it should be noted, entwines with the case law of the ECJ. In many cases, the Court has established the principle that data cannot be collected indiscriminately. *Inter alia*, Tele2 Sverige AB v Post-och telestyrelsen C-203/15 and SSHD v Tom Watson & Others C-698/15.

[119] For example, the proposed Code of Conduct on privacy for mobile health applications states that exact age should not be requested and stored if the same result can be achieve by a range age (e.g. 20-30 years old).

subject from non-sensitive data and to de-anonymise[120] and appropriate safeguards should always be present, as, using the words of the European Commission: “privacy is not a commodity to be traded. Rather, respecting privacy and guaranteeing the protection of personal data is a condition for stable, secure and competitive global commercial flows”.[121]

2.4.3 GDPR Principles: Archiving

The GDPR, in the aforementioned article 5(1)(b), sets forth the archiving exceptions. The rule is similar to the former directive, but a new exception for further processing has been added: archiving in the public interest. In addition, the approach has been radically changed as just as the implications. While the directive allowed a special regime for the above-mentioned exceptions[122] as long as “appropriate safeguards” were provided, although without further specifications on them, the GDPR integrates it with article 89(1).

Archiving links article 5(1)(b), 5(1)(c)[123] and article 9(2)(j), among others, by the idea of implementing “appropriate safeguards”, that are not limited to, but summarised by the most favoured safeguards of the GDPR: pseudonymisation. When pseudonymisation – or other safeguards – is implemented and the purposes are based on a EU or a Member State law, following all the conditions explained by recital 156, it is allowed to process data for a purpose that is different from the original one.

This is highly relevant for statistical cookies and, probably, for Big Data analysis on such data sets. Having found this solution, the GDPR tries allowing a data market, as long as safeguards are provided.

However, it is not clear if this idea would work: it has been argued that it is going to be helpful for historians and public archives, but most likely it will be a problem for companies, especially pharmaceutical companies, which can deploy cookie in health-related internet of the things, or institutes involved in scientific research, which is going to be interpreted in a broad manner as indicated by recital 159.[124]

[120] (O'Neil, 2016).

[121] (Mid-term review of a Digital Single Market Strategy for Europe, 2017)

[122] For example, article 11 of the Directive allowed to avoid communicating to a subject that data have been obtained from a different source than the subject.

[123] In this context, it is almost impossible to separate purpose limitation from data minimisation as the typical database, on which this exceptions apply, is remarkably vast. (Moerel and Prins, 2015).

[124] (Ustaran, 2018, pp. 154-155).

The WP29 – although in the context of the purpose limitation issue – proposed the notion of functional separation to address the data further processed in relation with archiving purposes. It means that the usage of such data must be intended to support measures and decisions with regard to an individual data subject, unless that subject has given his or her consent.[125] Assuming, *arguendo*, that such notion could become a fundamental point regarding what kind of safeguards must be deployed, both technical and organisational, the real and factual turning point is going to be the DPIA, *ex* art. 35 and, even more important, *ex* art. 36, the prior consultation with the Authority. In a scenario in which a controller wants to use the cookies data for marketing research – and that was not the declared purpose, when collected – it could be allowed as long as DPIA on appropriate safeguards finds that there have been implemented proper safeguards, the risks have been addressed and minimised or an explicit consent has been obtained.[126] Either way, the hope of a "ethical" data market is arguably going to become the ground for a legal claims.[127]

2.5 WP29 Opinions on Cookies

The (defunct) WP29 has addressed the issue of cookies from time to time. There are opinions related to cookies and other opinions that include cookies.

Two of the most interesting documents are Opinion 04/2012 on Cookie Consent Exemption and Working Document 02/2013[128] providing guidance on obtaining consent for cookies. They were elaborated to elaborate the consent issue introduced by the EPD.

It should be noted that cookies have also be mentioned in the Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC – which it referred to the Opinion 2/2010 on online behavioural advertising – and the WP29 noted that cookies cannot easily be deployed by a controller under the legitimate interest. The discussions involving cookies, two example provided: cookies used for electronic monitoring of internet use and for combination of personal information across web services, found out that cookies, due to their intrusive nature, violate principles of proportionality and transparency about the practices. Moreover, cookies do not

[125] Opinion 03/2013.

[126] (Culik and Döpke, 2017)

[127] Article 13(3) states that if a controller "intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2". It would be dubious, in the case of cookies, that a controller, by itself or through a processor, could fulfil this duty of information.

[128] It will be covered in the next chapter.

allow a user to effectively control the processing of the data (the specific combinations of their data across services and users cannot object to the combination of data), realising an imbalance between the legitimate interest and reasonable expectations of the data subject.

The opinion 04/2012 analysed when cookies are exempted from consent. It reaffirmed the two criteria of article 5(3) EPD and it explained them.

Regarding the cookies used "for the sole purpose of carrying out the transmission of a communication", it stated that there are three elements to establish what is "strictly necessary for communications to take place over a network between two parties": (i) the ability to route the information over the network, notably by identifying the communication endpoints; (ii) the ability to exchange data items in their intended order, notably by numbering data packets and (iii) the ability to detect transmission errors or data loss.

Therefore a cookie that is relevant for one of these three elements are encompassed by this criterion.

Regarding cookies "strictly necessary", WP29 elaborated two tests that must be passed: (i) the information society service has been explicitly requested by the user: the user (or subscriber) did a positive action to request a service with a clearly defined perimeter and (ii) the cookie is strictly needed to enable the information society service: if cookies are disabled, the service will not work. However, following recital 66 of Directive 2009/136/EC (the directive that emended the EPD), there must be a clear link between the strict necessity of a cookie and the delivery of the service explicitly requested by the user for applying the exemption. Such necessity must be examined by the user point of view.

WP29, applying these two criteria, found that third party cookies are almost never covered by the consent exemption. While, regarding multi-purpose cookie, the specific purpose must be taken into consideration: while the mere remembering of preferences is most likely to be covered, other activities of that cookie (like tracking) are not covered (and consent must be reached).

On one hand, cookies that are legitimately exempted by the consent are: user-input cookies (first-party cookies to keep track of the inputs: online forms, shopping carts and so forth), authentication cookies (to identify the user for the duration of a session), user-centric security cookies (for detecting authentication abuses), multimedia content player cookies (used to store technical data to play back video or audio content), load-balancing cookies (to handle the server connection and redirection), user-interface customisation cookies (language or font preferences) and third-party social plug-in content-sharing cookies (but only for logged-in members of a social network[129]).

[129] Consent of non-members should be achieved.

On the other hand, cookies never exempted are: first party analytics cookies[130], third party advertising cookies and social plug-in tracking cookies cookies.

Moreover, in the Opinion 02/2013 on apps on smart devices, it was reaffirmed that consent should be reached to avoid unlawful processing when free apps earned money by advertising, especially if contextual or personalised advertising is involved.

Summarising: first party cookies are the one most likely to benefit from the exemption regime.

2.6 The possible futures

Reaching a balancing between technology necessity and data protection is always complicated. The proactive solution of computer science could be beneficial, but only if a legislative action is covering the problems properly, which requires time that policy makers do not have in a fast changing world.

Today cookies are used, but tomorrow a new emerging technology could replace them. Therefore the level of abstraction, when considering this issue, should be flexible enough to be able to cover future development, in the limit of what is possible.

In this context, GDPR possesses different useful instruments.

The idea of privacy by design and by default could shape how cookies will be used in the next years, as long as the principles are defined.[131] Appropriate safeguards like the encouraged anonymisation and pseudonymisation. Conducting DPIAs and the presence of a DPO could try to mitigate the risks for users. Adherence to code of conducts, stimulating an undertaking to adopt one and therefore to develop a culture of privacy, certification-scheme, seals and international standard could play a role.

[130] These cookies does not necessarily fall outside the two criteria, as long as anonymisation and appropriate safeguards (e.g. opt-out) have been provided, but they are relevant for providing functionalities explicitly requested by the users: a user can access all the functionalities when analytics cookies are disabled.

[131] The European Commission supports the adoption of processing measures that are less intrusive, e.g. the request of an ID for identifying a data subject is less intrusive than biometric data, but how this could be relevant for cookies requires further specifications and guidelines.

Moreover, a company will always be under the sword of Damocles of sanctions. Not just the pecuniary sanctions of article 83, which are quite harsh, but the even worst possibility to receive an order to stop a processing, art. 58(2)(f).[132]

However, when cookies are involved not every solution is applicable: for example, minimisation cannot always be possible. The reliance on consent, which is central in the GDPR and not only, is arguably too optimistic as cookies outreach the average comprehension of a data subject.

The cookie issue cannot be solved out by looking for one simple solution. The possible path could be to gather all these possibilities and combine them, creating new way to approach how cookies are intended. But the great variable of EPR is still pending.

Most likely only promoting a culture of privacy will be successful in the long term.

[132] The GDPR tends to graduate the level of intervention of an Authority. Before harsh sanctions are imposed, warnings and reprimands should be sent, considering and evaluating the nature of the case.

CHAPTER III: Case law and current issues

3.1 Cookies and Consent

The legal topic of consent is one of the most famous in the history of modern law. Almost irrelevant for the Roman law, it became important since the “Dogma of Will” (*Willensdogma*) of the Pandectists has started influencing the European continental tradition. Today, the theories of consent elaborated in the Common Law systems have started taking roots too.

In the era of the Internet, consent is meant by the EU in a less speculative way: it was defined by the directive and now by the GDPR, article 4(11) along with article 7.

The first article states that consent[133] must be “informed, specific, freely given and must constitute a real indication of the individual's wishes”[134] and the second sets three important rules: the controller must prove that the data subject has consented, the request for consent shall be presented “in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language” – as punishment for violating this, such declaration is not binding – and the right to withdraw the consent at any time and without detriment. However, data processed under a valid consent are considered lawfully processed.

The GDPR does not provide formal requirements for the consent: it could be given by oral or written statement, including electronically. But the written form is the most convenient, as the burden of proof is born by the controller, who must demonstrate it, as a consequence of the accountability principle: art. 5(2).

These provisions are relevant even for the EPD (and in future for the EPR) as there is a reference on the topic between the two legal tools. However, it must be noted that, assumed the consent, the EPD has been implemented by the European Authorities in two different way: most of the Member States

[133] The idea of consent for processing information can even be found in article 39(2) of the Agreement on Trade-Related Aspects of Intellectual Property Rights: "Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices".

[134] It essentially the same definition, besides the words order and the syntactical construction, of the former directive: “'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed”.

allowed a generic opt-out, while a opt-in is strictly observed only in Germany[135], Italy, Netherlands and Croatia.[136]

This has led to required a clear affirmative action of a data subject[137], which could be ticking an unticked box on when visiting an Internet website or choosing technical settings, like selecting which cookies are allowed. On the contrary, silence, pre-ticked boxes or inactivity cannot be equated to consent. But this would imply that the opt-out model is therefore generally not permissible, unless it refers to the list of cookies exempted by the consent.

In the context of cookies, as specified by WP29[138], it entails:

Specific information must be provided: blanket (or bulk) consent without specifying what is the cookie purpose is not considered as acceptable. A web site is not obliged to provided all the information at once, but it could prominently display a link (so-called: “layered approach”) to a designated location where all the types of cookies used by the website are presented. Necessary information would be the purposes and, if any, details of third parties cookies (or third party access to data collected by the cookies on the website), retention period, typical values and other technical information. The users must also be informed about the ways they can signify their wishes regarding cookies i.e. how they can accept all, some or no cookies and to how change this preference in the future.

It should be given a time to agree, as a general rule, consent to cookies has to be given before the processing starts. Therefore to comply with this consent should be sought before cookies are set or read. It means that, when using cookies that are not covered by consent exemptions, a website should deliver a solution in which no cookies are set before that user has signalled the wishes regarding such cookies.

If consent must be “unambiguous”, the procedure should not leave space for doubt about the intentions. This means that any kind of active choice or signal, sufficiently clear to be capable of indicating a data subject's wishes, and to be understandable by the data controller (the aforementioned affirmative action)

[135] It can be interestingly noted that Germany has not transposed of the EPD, as the old telecommunication law was considered by the Commission as sufficient: it went only through a revision process, for including special cases like profiling.

[136] Some authors have suggested that such proliferation of opt-out is just a consequence of a lack of determination of Authorities. *Inter alia*: (Gutwirth, Leenes and De Hert, *idem*)

[137] For a detailed in-depth about the concrete systems: (Utz et al, 2018, p. 8)

[138] Working Document 02/2013 providing guidance on obtaining consent for cookies.

Last, it should be freely given. A consent, to be considered valid, must be givien by a data subject that can freely exercise a real choice: deception, intimidation, coercion or significant negative consequences are not considered able to produce a valid consent. For example, if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment. However, recital 25 of EPD allows that the access to specific website content may be made conditional on the well-informed acceptance of cookies (if it they are used for a legitimate purpose). But, as WP29 noted, the emphasis is on "specific website content" which entails that websites should not condition "general access" to the site on acceptance of all cookies. It can only limit certain content: for e-commerce websites, whose main purpose is to sell products, not accepting (non-functional) cookies should not prevent a user from buying products on this website. Additionally, according to recital 10 of EPD, storing information or gaining to the information already stored can entail the processing of personal data and therefore data protection rules clearly apply.

In an attempt to simplify these requirements, the European Commission has developed a cookie consent kit, freely downloadable from its website.

3.1.2 Browser settings

Another possibility to express a consent is through the browser settings.

This possibility is derived from recital 17 of EPD, which lays down that consent "may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes". One method could be browser settings.

This possibility has been criticised by the WP29 at the time of its introduction[139], because the problem was that from one point of view browser setting were too permissive in accepting cookies and, from another point of view, it could have been easily eluded by Flash cookies.

However, the WP29 stated that a compliant default policy would be to reject third party cookie, which should be actively accepted by a user. Moreover, browser settings do not relief from providing information to a user, especially in regards of the cookie purpose.

The WP29 also proposed the introduction of a "privacy wizard" that should guide a user through the privacy configuration. This proposal, which was seen as an implementation of privacy by design

[139] (Kosta, *supra* at 397-399)

principle, has never been totally developed: browsers usually come with the operative system and even when the default browser is not used, the new one is not totally implementing a privacy wizard (at least, this is not the case of Firefox, Chrome or Internet Explorer). A user is usually invited to set the privacy settings, but it is not mandatory and it can be postponed.

If the stricter rules of article 10 of EPR survive, this possibility is foreseeable to become a relevant standard for consent.

3.1.3 Other systems

Other ways to express a consent, analysed by the WP29, are the pop-up windows that present relevant information to users. This system has been considered compatible with a "clear and comprehensive way" of offering information.

Another possibility could be a "splash screen", which forces the users to read the relevant information when opening the web site. If this works in practice, it is doubtable: when presenting a splash screen a user will either go away or accept anything to access the website.[140]

Last, numerous ad-blockers, anti-trackers and do-not-track headers have been made available to the public by privacy-concerned groups or people. The issue of them has not been covered by the WP29 and, hopefully, it will be by the EDPB. In the current situation, they can be seen as compliant with recital 17: it is a clear way, through browser add-ons, which can be considered a more refined setting, to express indication of the user's wishes.

Without further clearance on this possibility, these systems clash against the business policy of the over-the-top.

An interesting example is that Google do no allow on Chrome the ad-blocker AdNauseam, which does not just block third parties cookies, but it randomly "clicks" on advertising in order to invalidate statistical and behavioural analysis.[141]

[140] (Kosta, *supra* at 400-401)

[141] (Kosta, *Ibid.*), for a critical examination of the transposition in Netherlands: (Kosta, 2016)

3.1.4 Is a well-informed consent possible?

Until now, the issue of cookies has been solved out through rules and specification about what kind of information should be provided and how a consent should be reached.

The approach was necessary, but it does not remove all the problems that cookies imply and entail.

Cookies are not just something that can be addressed, but part of the problem itself. For example, Google has a "CONSENT" cookie that saves the consent given to Google policy. It can be seen as strictly necessary: without giving the consent to Google, the search engine and its products cannot be used, due to its technical implementation. Moreover this cookie is generated only after a user has decided whether accepting or not the general terms and conditions, which include provisions about cookies.
However, if a user is logged-in and the "CONSENT" cookie is deleted, it is irrelevant for Google – and maybe it can be respawned as it is strictly necessary and therefore it does not required a consent – but at the same time, deleting that cookie is a clear affirmative action.

The example is debatable, but it shows while an excessive reliance on consent should be better understood: an average user wants to enjoy the internet and does not care about technical processes that happen without the user's awareness.

In traditional civil law, this is already known: it is similar to a contract of adhesion. In that case, a (weak) party finds a contract and its terms and conditions already written by the other (strong) party and it is not negotiable. The policy maker's – national and European – reply to this situation was quite strong: the creation of the idea of consumer, because it was recognised that the consent was, on some extent, less freely given than wanted.

In the data economy context, the policy maker seems to forget how to reply in a decisive manner and prefers to ignore that consumer protection could find room to manoeuvre. It was (partially) the idea behind GDPR (and EPR): sanctions that can be effective, borrowed from consumer protection (but without the power to break monopolies[142]).

At the same time, informing a user shows many limits: spreading banners across the web or forcing users to click on cookie buttons has a limited relevance for what concerns the actual knowledge of how data are processed. Most of the information is not so easy to understand due to the highly

[142] The Dutch broadcaster fined for having violated the consent mechanism was fined for just 25000 Euro, which is clearly ridiculous in comparison to consumer protection law. In Dutch: (Nu.nl, 2018)

complicated nature of how they are processed and the average user could not be interested in reading either over-generalised terms – which tell nothing, but they do it in a clear and plain language[143] – or pages of complicated legal jargon.

At the current stage, it cannot be imagined that users are aware of the cookie issue and not often by their fault: one of the duty of information is to make clear who is the data controller. This requirement is often disregarded, both for first party cookies[144] and especially for third party cookies, where is should be fundamental.[145]

Furthermore, in the recent ECJ case[146], which involved the use of analytics cookies, namely the Facebook Insight system, the Court ruled that Facebook and the Page Administrator were (joint) controllers, although with a different degree of liability. Following this judgement, the allocation of responsibility, when third party cookies are involved, would be extremely beneficial for users, but not for business.

In conclusion, the problem of consent and cookies is far from being solved and, unless the approach radically changes the problems will just become the proverbial elephant in the room.

3.2 GDPR rights and the zombie problem

It was March 2010 when the European Data Protection Supervisor, in its "Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy", suggested that flash control should be integrated in browsers.[147] It was a reaction to a 2009 Paper that pointed out the risks of flash cookies as well as to the 2010 settling of a lawsuit related to zombie cookies usage by Quantcast.[148]

The issue was not noticed for some years, until in 2015, when an advertising company, called TURN, exploited a hidden number – used by Verizon[149][150] to monitor users' behaviour on their

[143] Google was fined for installing cookies without consent, under a not well-defined policy and failing to inform the users: (Le Moullec, 2014)

[144] Facebook was fined by Belgian Authority for failing to inform the users of a changing in terms and condition in which allowed its cookies to track users through the web: (Ducuing, 2018)

[145] In the first half of 2018, in French a fine was imposed for this reason: (Lebeau-Marianna and Chancé, 2018)

[146] *Wirtschaftsakademie Schleswig-Holstein GmbH v. Facebook Ireland Ltd*, C-210/16 of June 5th 2018

[147] This has led, for example, in Internet Explorer and Firefox, to ask permission to run Adobe Flash plug-ins.

[148] (Singel, 2010; Crawford, 2013)

[149] AT&T used a similar identification. But when they stopped when complains started.

[150] In this case, it is dubious that Verizon did not know about TURN's activities as the connection between the two companies was proved.

terminals – to respawn tracking flash cookies that users thought to have deleted.[151] After the case was brought to the public, TURN claimed to have stopped these activities.[152]

The European Institution was quite competent in foreseeing the issue: flash cookies are a problem for privacy. If the level of intrusion is analysed under the GDPR principles and rights, it can be easily note that many problems arise.

Zombie cookies violated directly at least lawfulness, fairness, transparency and storage limitation principles and the right to erasure and restriction to processing.

When evercookies are stored, the users are neither informed nor a consent is obtained. The cases showed that when they are implemented it is done without a public notice, violating all provisions on transparent communication. As consequence, it also leads to a lack of a legal basis – both under GDPR and EPD – as no legitimate interest can be claimed (and the WP29 has turned down such argument for less invasive form of cookies). Furthermore, if a cookie is deleted, the withdraw from the previous consent is affirmed. But zombie cookies recreates themselves identical: without a new request for consent, they are forcing a user to accept (without knowing) cookies that have not been agreed upon.

Even if it is assumed that they are strictly necessary cookies, the situation is not ameliorated. The two criteria for establishing when a cookie is exempted from consent would not apply: zombie cookies can recreate themselves outside the initiation or maintenance of carrying out a communication and they fail to pass the two test for necessity: they have neither been requested by a user nor they are necessary to provide a services, because they realise an imbalance that cannot overrun other fundamental rights, especially when there are other less intrusive ways to manage that.

Last, if WP29 has been rejected that hundreds of years is a reasonable time for storing cookies, zombie cookies are virtually forever. This entails that they do not even apply a data retention policy: they just survive.

Regarding the rights, the fact that they respawn can be considered as violating the right to be forgotten, which is the right of every subject to have the data erasured. Specifically they meet at least four of the situations indicated by art. 17(1).

When a zombie cookie is deleted for the first time, it can be considered a withdraw of the user's consent and, therefore, lacking any other ground (especially under EPD rules), 17(1)(b) is met. But

[151] (Angwin and Tigas, 2015)
[152] (*Idem*)

simultaneously the cookie recreates itself without the consent: every data processed from that moment is *ipso facto* an unlawful processing, art. 17(1)(d). Moreover, depending on where this happens, a Member State's data retention policy applies. If it prescribes that such data must be deleted, it is also a violation of a legal obligation, art. 17(1)(e).

Could a company enjoy the exceptions listed in article 17(3)? None of them[153] seems to apply to zombie cookies.

The only possibility could be the letter (b): "compliance with a legal obligation" or "performance of a task carried out in the public interest". But even in this case, it could be difficult to argue that zombie cookies are the best way to achieve such compliance: such means would most likely lack the proportionality required. Zombie cookies are extremely intrusive and persistent and they go far beyond what could be requested, for example, for lawful interception. In the presence of other means, for example just saving the IP address, evercookies seem also not to be necessary to comply with a legal obligation.

Last, article 18 gives the right to a data subject to have a processing restricted if at least one of the condition enumerated applies. Namely, after the first deletion, zombie cookies result in an unlawful processing, art. 18(1)(b).

Following this, the controller cannot rely on the processing of the data obtained any further, with the exception of storage, without the consent (assuming that at the first storing zombie cookies had been lawful). But considering the issue, this would be able to aggravate the controller's situation if a fine is imposed.

Probably, if there have been no relevant case about zombie cookies, it is a direct consequence of this general data protection principles and rights.

[153] The establishment of a legal defence is also not arguable a base. What would be the reason for keeping saving a user's data, when such data are already in the availability of the controller?

CHAPTER IV: Cookies in the Big Data Era

The phrase “Big Data” has become quite famous in the last years. The idea is that a large and kaleidoscopic scale of data, is analysed in almost real time, using peculiar techniques, to extract different and unpredictable information, correlations and patterns. The essence of Big Data is the so called three Vs: Volume, Variety and Velocity.[154]

Cookies can play a role in this Big Data context: they allow the creation of a data set, with many different data and they can transmit them in real time (although the analysis will not be conducted by cookies themselves.

From a legal point of view, this is one of the most challenging issue. The GDPR has tried setting some rules to solve it out.

4.1 Automated decision-making and profiling

Article 22 of the GDPR, which is related to automated individual decision-making tools, is not directly relevant for cookies. But it is the integration of cookies with automated decision-making systems to pose high risks.

Data analysis can be as much accurate as it can infer wrongly, but, when this false statistical inferences produce legal effects or “similarly significantly affects”, it can lead to illegitimate or discriminatory results. This risk may increase exponentially if the data set is not up-to-date.[155] The consequences of this scenario could be an increment of social exclusion for some categories, e.g. if the system decides weather a subject can obtain a loan or an insurance.

The GDPR introduced the article 22 as an attempt to mitigate such situations. The article, which is a prohibition masqueraded by right[156], sets forth that a subject cannot be subjected only to an

[154] (Corrales, Fenwick and Forgó, 2017, pp. 20-22)

[155] Such situation would be both a breach of the obligations under article 22 and article 5(1)(d), the principle of accuracy. Furthermore, it is unluckily that a data subject could be aware of every single data that has become outdated, in order to exercise the right to rectification (article 16).

[156] *Inter alia*, see (Bygrave, 2014)

automated decision, unless one of the three exceptions of paragraph (2) applies.[157][158] Two of these exceptions are subjected to a human intervention, among others "suitable measure to safeguard data subject's rights and freedoms", according to paragraph (3).[159]

This article must be read in accordance to the dispositions of articles 13(2)(f) and 14(2)(g), which set forth a duty to provide "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject".

This provision is not an absolute right and it should follow two *caveat*: recital 63 and the further specification of EDPB.

The first one pertains to the reasonable expectations of the controller, that is not obliged to disclose "trade secrets or intellectual property and in particular the copyright protecting the software", but only to provide a summary. In this way, GDPR tries balancing between commercial interests and data protection.

The second specification is related to the position of a data subject that has the right to be provided with "meaningful", for him or her, information and in a "simple way".[160] Additionally, complexity cannot be invoke as an excuse for not being able to fulfil the latter provision.[161]

As the GDPR will not apply just to future processing, all data that companies have already gathered – which constitute quite consistent data sets – ought to be processed according the obligations therein.[162] Cookies are the basis that allowed those and, therefore, Big Data activities.

4.2 Profiling

A peculiar case of automated processing, even mentioned in article 22, is profiling.[163]

[157] (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent.

[158] Article 22(4) prescribes for the special categories of data outlined in article 9(1) only two specific derogations are allowed: explicit consent and public interested.

[159] Letter (a) and (c). This can be considered as one of the many example of poor legal writing style of GDPR.

[160] Guidelines on Automated individual decision-making, p. 25

[161] *Ibid*.

[162] (Datoo, 2017)

[163] This work will limit the discussion to the commercial aspects of profiling. For a technical discussion about how cookies have been used by NSA see (Cerquitelli, Quercia and Pasquale, 2017, pp. 55-58) and for a more comprehensive work on cookies and surveillance (Norris et al, 2017).

The WP29, elaborating the definition included in article 4(4) of GDPR[164], has explained that Profiling has three main elements: it has to be an *automated* form of processing; it has to be carried out on *personal data*; and the objective of the profiling must be to *evaluate personal aspects* about a natural person.[165][166]

Regarding the evaluation of personal aspects, recital 24 particularly lays down that it must be verify if it concern the prediction of “personal preferences, behaviours and attitudes”. As it is imaginable, profiling – which is can be based on cookies[167] – can lead to even more contingent outcome, when used. Although not every kind of profiling could be harmful, but nothing is said about such kind of processing.[168]

For that, the GDPR mentions it in article 35(3)(a) as one of the three cases in which a DPIA, “shall particularly be required”. The DPIA is not only a guarantee to data subjects, but as explained by recital 91, a useful tool of accountability and interaction with public authorities.[169] In the context of cookies, it is an almost mandatory obligation, when intrusive cookies are used.

Moreover the sensitive nature of profiling has produced the recital 72, that explicitly mentioned that “profiling is subject to the rules of this Regulation” and the EDPB “should be able to issue guidance in that context”.

What does it means that profiling is subjected to the GDPR? The scope of the recital was not to narrow profiling only to article 22. When profiling is involved, a controller shall allow data subjects to exercise every right, from article 15 to 22.

Furthermore, as stated by recital 60, elaborating fairness and transparency, a controller must inform a data subject “of the existence of profiling and the consequences of such profiling”.[170] Thus allowing a data subject the possibility to enjoy a broad protection. But if this is concretely done in cookie policies, it is doubtable.

[164] “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 analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements”.

[165] *Ibid*. pp. 6-7

[166] "Natural Person", in case of profiling, means only an adult, as recital 71 excludes profiling of children.

[167] Recital 30.

[168] One possible solution could be to request an evaluation based on the nature of innocuous processing. Another could be related to the expression of article 22(3) “rights and freedoms and legitimate interests” and the resulting analysis.

[169] Although the GDPR tries to strengthen the cooperation of the 28 Authorities in the European Union, through, for example, the consistency mechanism, it doubtful or at least problematic that, in case of Big Data, a successful cooperation would be accomplished: a factual inspection through the European Union could be stopped by linguistic problems, different rules on how to conduct it or, simply, reticence.

[170] Such information can be provided in different way, for example "in combination with standardised icons" (standardised by the European Union), "in an easily visible, intelligible and clearly legible manner" or in "a meaningful overview of the intended processing".

Last, other important provisions are contained in recital 71.

The recital, stressing the risks of automatic processing, including profiling, suggests, in order to avoid detrimental situations, "implement technical and organisational measures appropriate to ensure [...] that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks [...] and that prevents, *inter alia*, discriminatory effects".

Therefore, cookies involved in profiling, in the context of GDPR, would be, even in this case, a matter of the appropriate measures undertaken.

4.3 Behavioural Targeting and Tracking

Cookies, especially third-party, are important for providing target marketing.[171] In order to reach an effective target marketing, there related cookies must be involved in behavioural targeting and tracking. Not just cookies, but many different techniques.[172]

Advertising consists of two technical parts: on one hand it must be decided what ad should return in response to a request and the actually sending of it. This is usually conducted via third-party cookies, which allow targeting more precisely. But eliminating such cookies would not neither prevent an advertising network from returning an ad nor eliminate the profiling of users, only profiling done by third parties (Smith R., 2001, cited in Kristol 2001).

If a web site uses its own ad scan, it can still profile and target visitors, using its own cookies. The results would be, most likely, less effective,

The issue of cookies for behavioural analysis have brought to one famous case in America: a series of class action lawsuits brought against DoubleClick[173] for violation of privacy[174], especially relating to the company's cookie tracking practices.

One year later, in August 2011, Microsoft, on its website, was discovered having implemented flash supercookies and, only in the aftermath, they disabled them.[175]

[171] (Hoeren and Kolany-Raiser, 2018, pp. 74-76)

[172] (Tene and Polonetsky, 2012, pp. 245-249)

[173] In re DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001)

[174] It must be noted that DoubleClick was found not guilt in regards to the Stored Communications Act, the Wiretap Statute and the Computer Fraud and Abuse Act. For the complete legal arguments: (Hang and Chadwick, 2004)

[175] (Mayer, 2011)

An interesting reaction that came from American was the development of principles, for dealing with transparency. They are self-regulatory principles and they have been developed by the Digital Advertising Alliance in America. Many other associations have been established worldwide for this scope, *inter alia* the Network Advertising Initiative and, in Europe, the European Interactive Digital Advertising Alliance.

In a GDPR context, it is assumed that, once a company complies with the general provisions, behavioural marketing is legitimate.

However, the supercookies pose problems: they are very invasive trackers. But the regulation does not provide for special rules, as, if appropriate safeguards and data protection principles are not implemented, it relies on sanctions to stop the processing and impose pecuniary sanctions.

From a user point of view, encryption and secure communication tool (such as Virtual Private Network, peer-to-peer communication, onion routers) should be taken into account. But they have clear limits: slow connection and, once a user is forced to log-in, it can be tracked.

A more interesting proposal, which would be a possible compromise, could be to promote European companies[176] for target advertising that would respect GDPR principle and would engage in targeting based on statistical analysis or small data (Lindstrom, 2016[177]). In this way, it could be assured a balacing between data protection and business legitimate expectations.

4.4 Cookie Policies

Last, after having considered all the legal instruments and rules in Europe, a brief analysis of the most used web site could be beneficial

4.4.1 Google and YouTube

[176] (Fan, 2017)

[177] The concept of Small Data is about a data set based on format and volume that is understandable by a ordinary human being (e.g. observations of one's everyday life, cultural information or diet). That can lead, through creativity and understanding of causation, to a more practical and relevant solutions. The starting point for this Small Data is still a Big Data analysis (i.e. machine-made) which is able to find out correlations in an immense data set, but only to reduce it to a more intelligible form (for humans).

The policy of Google[178] is introduced by a 4:30 long video, which is quite generic. The policy itself is generic too, although some examples of cookies used are provided and it included, at the top, a link to handle cookies, which is not so useful (it just explains what to do and it is not mobile-friendly).

There is no complete list of the used cookies, with the exception of the domain used for advertising. Purposes are indicated and sufficiently described, but they lack of detailed indication about retention policy. Regarding advertising cookies the information is quite detailed, more importantly there is a direct link to Google setting for this cookies.

On the other hand, there is specific link for analytics cookies and this is complete: values, purposes, retention and many other technical informations. The general policy should try copying this one.

It should be noted that, ironically, the cookie policy of Alphabet Inc., the conglomerate that owns Google, is actually complete and compliant.

4.4.2 Amazon

The cookie policy of Amazon[179] is an example of a corporation that has not implemented a good policy.

Amazon, who is facing a current privacy data breach[180], has a cookie policy that is too short, generic and mostly useless.

Purposes are shortly described, without any indication of values and retention. The only list is the one related to third-party cookies[181], but the advertising cookie management is not linked in the policy: for finding it, one must open the general description of the internet-base ads and, at the bottom, there is a link to the actual preferences.[182]

The cookies notice links to the general privacy notice for an in-depth analysis. This policy seems too long, legal and complicated: for example it gives too much information about international data transfer, when some short indication would be enough, provided an *ad hoc* linked page.

[178] (Google, 2018)
[179] (Amazon, 2018a)
[180] (Emont and Stevens, 2018)
[181] (Amazon, 2018b)
[182] When it states that cookies can be manage trough a user’s account, it just link to the account homepage and not to the appropriate management system.

It would be advisable for Amazon to change its cookies policy on the Google analytics cookie model or, even better, on the Facebook model.

4.4.3 Facebook, WhatsApp and Instagram

On the contrary, Facebook policy, probably due to the periodic scandals that hit the company, is one of the best among the over-the-top.

It is well layered and contains everything: all the values, the purposes and the retention policy. It links properly the legal page for processing and all the third-party are listed.[183] There are links that redirect to the appropriate page to manage cookies and advertising as well as privacy in general. Even more interesting is that it links to three important international organisations for handling advertising: Digital Advertising Alliance (United States), Digital Advertising Alliance of Canada and European Interactive Digital Advertising Alliance. Last, it suggests to set preferences via browser settings.

While Facebook as an admirable policy, its subsidiaries do not follow this example.

WhatsApp[184] has a cookie policy inserted in a long “legal info”, that included privacy and other information, and it is posed at the end. It is very short, wide and generic. No value, no retention and the purposes are incomplete. There is no further link to manage cookies, but only a general instruction about how to do so. Third-party and advertising cookies are not mentioned, although in the privacy notice is stated that advertising messages are included in the services.

This could be another example of a bad policy.

At the same time, Instagram[185] has a policy more similar to the WhatsApp one than to the Facebook’s. Values and retention are not indicated and purposes are generically described. There is not no list of third-party cookies, which is always a violation of the duty to provider the controller details. There are instructions about where to find the advertising settings, but no link. However there are links to the aforementioned international associations.

[183] It is curious to note that Wikimedia Foundation implements the same cookies, when an article is share, that Facebook does.

[184] (WhatsApp, 2018)

[185] (Instagram, 2018)

4.4.4 Twitter

The policy of Twitter[186] is peculiar example of policy: it is well-written, not too complicated, it proves good example for purposes, which are fairly described. However, it misses values and retention.

It is however interesting to note that the policy is strongly integrated with Google policies for that concerns advertising and analytics, but, if there are other marketing partners, the list is missing. Nevertheless, it also provided useful links to manage the settings of every relevant issue (cookies, ads and third-party). The link to personalisation of the service, when logged-in, is differentiated (by a light-grey colour).

However, it would be advisable to integrate the missing information in order to fully comply with the European regulations and directives.

[186] (Twitter, 2018)

CONCLUSIONS

The issue of cookies is not a piece of cake.

The legal framework is quite fragmented and the EU, where a certain degree of harmonisation was sought trough the EPD, needs to shift to more simple and (hopefully) strengthened rules. Such is promised by the EPR, but political will or pressing lobbying is slowing down and, maybe, compromising the lawmaking.

Many solutions have been proposed, but some of them – sanctions, like order to stop a processing activities, fined and even criminal law, when implemented[187] – would be just a reaction. But a reaction, in this context, is not able to restore the balance between the parties: once a dataset has been acquired, it can be simply exploited in secret. The recent case of Google, buying a data from Mastercard[188], is clear signal of how privacy can be ignored even in a post-GDPR world.

The best approach, generally speaking for privacy, but especially for topics like cookies, is a proactive one.
Privacy by design and by default are a very good starting point: they allow users to live in a safe environment without the need to spend too much time caring about the issue. But strong action is not advisable to be undertaken without public discussion and consultation of all the possible stakeholders: the question if an hardware producer should be involved in this privacy-by process could just lead to abandon known technologies to develop new ones, which would slow down the regulative process.[189]

Moreover Do-Not-Track headers, ad-blockers and anti-trackers shall have their legal status clarified as soon as possible as they can play an relevant and important role.

Limitation on some form of malicious cookies should be implemented, especially for supercookies and zombie cookies, and one of the best way to to it is through the develop of clear rules for browser settings to deal with cookies (in general, but specifically for Flash cookies).

For what concerns the marketing aspects of cookies, an interesting metaphor is offered by the famous tv series Black Mirror, episode “White Christmas”. In which there is device called “cookie” which is able to micromanage the life of the owner, controlling the electronics around the owner.

[187] Among others, Italy and Austria apply criminal sanctions in the field of Data Protection. For a complete list: (Bird & Bird, 2018)

[188] (Bergen and Surane, 2018)

[189] Opinion 05/2018, p. 14

The device, which is just a small empty egg-like object, contains a digital copy of the owner. It is a perfect metaphor of what a marketing cookies are: the data transmitted are pieces of a person. Fragments and shreds of a life that, when put together, have an incredible power, for legitimate and illegal purposes, ranging from surveillance to behavioural tracking. It is important in this context not just to promote a privacy culture, but also to involve different associations for these specific topics, due to the best level of control that they can exercise on the corporations and the possibility of class action now included in the GDPR.

Summarising, there are many possibilities, but the time is limited. GDPR has produced an incredible impact, but it was possible mainly due to the Snowden revelations. If, in this absence of a cookie massive scandal, this would lead to a change, can only be hoped.

BIBLIOGRAPHY

BOOKS AND ARTICLES

AliceWyman – away et al (2018) "Cookies - Information that websites store on your computer" [online]. Available at: https://support.mozilla.org/en-US/kb/cookies-information-websites-store-on-your-computer (accessed: 10th June 2018)

Angwin, J. and Tigas, M. (2015) “Zombie Cookie: The Tracking Cookie That You Can't Kill” *Pro Republica*, 14 January [Online] Available at: https://www.propublica.org/article/zombie-cookie-the-tracking-cookie-that-you-cant-kill (accessed: 10th June 2018)

Aycock J. (2011) *Spyware and Adware*, New York: Springer Science+Business Media, pp. 116-117

Backes M. et al. (2012) “ObliviAd: Provably Secure and Practical Online Behavioral Advertising” *IEEE Symposium on Security and Privacy 2012*, [Online]. Available at: https://ieeexplore.ieee.org/document/6234417/ (Accessed: 10th June 2018) pp. 260-263

Barth, A. (2011) "RFC 6265" [online]. Available at: https://tools.ietf.org/html/rfc6265 (Accessed: 10th June 2018)

Bergen, M. and Surane, J. (2018) “Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales” *Bloomberg*, 30 August [online]. Available at: https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales (accessed: 1st September 2018)

Bond, R. “The EU E-Privacy Directive and Consent to Cookies”, *68 Bus. Law.* (215:12), pp. 220-223

Bygrave, L. A. (2014) *Data Privacy Law: An International Perspective*. London: Oxford University Press

Carmi, E. (2017) 'Regulating behaviours on the European Union internet, the case of spam versus cookies' *International Review of Law, Computers & Technology*, vol 31, no. 3, pp. 289-307

Cerquitelli, T., Quercia, D. and Pasquale, F. (2017) *Transparent Data Mining for Big and Small Data* [ebook] Springer International Publishing, pp. 55-58

Chen H. and Sivakumar T. V. L. N. (2005), "Access Control for Future Mobile Devices" IEEE Wireless Communications and Networking Conference 2005 [online] Available at: https://ieeexplore.ieee.org/document/1424741/ (Accessed: 10th June 2018)

Cormack, A. (2017) "The Draft ePrivacy Regulation: No More Lex Specialis for Cookie Processing", *14 SCRIPTed* (345:17)

Corrales, M., Fenwick, M. and Forgó N. (2017), *New Technology, Big Data and the Law*, 1st edn [ebook] Springer Nature Singapore, pp. 20-22

Crawford, D. (2013) "Supercookies, Flash cookies, Zombie cookies and things that go bump in the night" *BestVPN*, 10 December [online]. Available at: https://www.bestvpn.com/guides/super-cookies-flash-cookies/ (accessed: 1st September 2018)

Culik, N. and Döpke, C. (2017) "Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen", ZD: 226-230.

Datoo, A. (2017) "GDPR and Big Data – Friends or Foes?" *Gdprreport*, 24 July [online] Available at: https://gdpr.report/news/2017/07/24/gdpr-big-data-friends-foes (Accessed: 26th August 2018)

Dabrowski, A. et al. (2016) “Browser History Stealing with Captive Wi-Fi Portals”, *2016 Symposium IEEE Security*, available at DOI: 10.1109 (Accessed: 10th June 2018)

Ducuing, C. (2018) “Cookies and other (illegal) recipes to track internet-users: latest episode of the Facebook saga” *CiTiP Blog*, 8 March [online]. Available at: https://www.law.kuleuven.be/citip/blog/cookies-and-other-illegal-recipes-to-track-internet-users-latest-episode-of-the-facebook-saga/ (accessed: 1st September 2018)

Densmore, R. R. (2013) *Privacy Program Management: Tools for Managing Privacy Within Your Organization*, 1st edn, IAPP, p. 19

Eckersley, P. (2010) “How Unique Is Your Web Browser?” Electronic Frontier Foundation [online] Available at: https://panopticlick.eff.org/static/browser-uniqueness.pdf (accessed: 12th July 2018)

Emont, J. and Stevens L. (2018) “Amazon Investigates Employees Leaking Data for Bribes” *The Wall Street Journal*, 16 September [online]. Available at: https://www.wsj.com/articles/amazon-investigates-employees-leaking-data-for-bribes-1537106401 (accessed: 17th September 2018)

Fan, T (2017) “In the Future, Chinese People Will Sell Their Data For Cash” *Sixth Tone*, 14 July [Online] Available at: http://www.sixthtone.com/news/1000522/in-the-future%2C-chinese-people-will-sell-their-data-for-cash (accessed: 11th Julyt 2018)

Fazlioglu, M. (2018) “The top five contested issues in the EU’s developing ePrivacy Regulation”. *IAPP*, 3rd January [online]. Available at: https://iapp.org/news/a/the-top-5-contested-issues-in-the-eus-developing-eprivacy-regulation/ (accessed: 27th June 2018)

Fielding, R. (2014) "RFC 7230" [online]. Available at: https://tools.ietf.org/html/rfc7230 (Accessed: 10th June 2018)

Garnica, G. (2018) *Oracle WebLogic Server 12c Administration I Exam 1Z0-133: A Comprehensive Certification Guide*, 1st edn, New York: Springer Science+Business Media

Gutwirth, S., Leenes, R. and De Hert, P. (2016) *Data Protection on the Move*, 1st edn, Dordrecht: Springer Science+Business Media, pp. 214-215

Hang, L. and Chadwick, J., (2004) "Internet Privacy: A Tale of Two Cookies, *33 Brief* (48:04)

Hijmans, H. (2016). *The European Union as Guardian of Internet Privacy* [ebook] Springer International Publishing Switzerland, p. 497

Hoeren, T. and Kolany-Raiser, B. (2018) *Big Data in Context* [ebook] Springer, pp. 74-76

Hoofnagle C. J. et al., "Behavioral Advertising: The Offer You Cannot Refuse" *Harvard Law & Policy Review* (273:12) [Online] Available at: https://www.ftc.gov/system/files/documents/public_comments/2015/10/00048-97807.pdf (Accessed: 10th June 2018), pp. 281-282

Holman, W. J. Jr. (2018) "The Zuckerberg Effigy", *The Wall Street Journal*, 10 April [online]. Available at: https://www.wsj.com/articles/the-zuckerberg-effigy-1523399143 (accessed: 10th June 2018)

IT-Pol (2018) "EU Council considers undermining ePrivacy", European Digital Rights 25 July [online]. Available at: https://edri.org/eu-council-considers-undermining-eprivacy/ (accessed: 1st August 2018)

Lebeau-Marianna, D. and Chancé C. (2018) “France: Website publisher fined for violation of the cookie requirements” *DLA Piper Blog*, 11 July [online]. Available at: https://blogs.dlapiper.com/privacymatters/france-website-publisher-fined-for-violation-of-the-cookie-requirements/ (accessed: 1st September 2018)

Le Moullec, M. (2014) “The French Data Protection Authority Fines Google for Breach of French Privacy Laws” *Data Privacy Blog*, 31 January [online]. Available at: https://privacylaw.proskauer.com/2014/01/articles/online-privacy/the-french-data-protection-authority-fines-google-for-breach-of-french-privacy-laws/ (accessed: 1st September 2018)

Lindstrom, M. (2016) *Small Data: The Tiny Clues that Uncover Huge Trends*, 1st edn, St Martin's Press

Liu A. X., Kovacs J. M. and Gouda M. G., (2010) “A secure cookie scheme”, *Computer Networks* (56:12), pp. 1724-1728

Kamkar S. (2018), “Evercookie” [Online] Available at: https://samy.pl/evercookie/ (Accessed: 10th June 2018)

Kosta, E. (2013) “Peeking into the Cookie Jar: The European Approach towards the Regulation of Cookies” *International Journal of Law and Information Technology* (21:4)

Kosta, E. (2016) “The Netherlands: The Dutch Regulation of Cookies”, *2 Eur. Data Prot. L. Rev.* (97:16)

Kristol, D. M. (2001), HTTP Cookies: Standards, Privacy, and Politics [online]. Available At: https://arxiv.org/pdf/cs/0105018.pdf (Accessed: 10th June 2018)

Mayer, J. (2011) "Tracking the Trackers: Microsoft Advertising", *The Center for Internet and Society*, 19 August [online] Available at: http://cyberlaw.stanford.edu/blog/2011/08/tracking-trackers-microsoft-advertising (accessed: 1st September 2018)

Meyer, D. (2017) “Inside the ePrivacy Regulation's furious lobbying war”, *IAPP*, 31st October [Online] Available at https://iapp.org/news/a/inside-the-eprivacy-regulations-furious-lobbying-war/ (accessed on 11th July 2018).

Meyer, D. (2018), “ePrivacy rapporteur furious over Austria's limited ambition”, *IAPP*, 31st July [online]. Available at: https://iapp.org/news/a/eprivacy-rapporteur-furious-over-austrias-limited-ambition (accessed: 6th August 2018)

McDonald A. M. and Cranor L. F. (2012) “A Survey of the Use of Adobe Flash Local Shared Objects to Respawn HTTP Cookies” *ISJLP* (7:3), pp. 640-642

Moerel, L. and Prins, C. (2015) “On the death of Purpose Limitation”, *IAPP* 2 June [online]. Available at: https://iapp.org/news/a/on-the-death-of-purpose-limitation/ (accessed: 23th June 2018)

Mozilla Foundation (2018), "About Firefox Add-ons" [online] available at: https://addons.mozilla.org/en-US/about (accessed: 10th June 2018)

Naranjo, D. (2017) “E-Privacy Regulation: Good Intentions but a Lot of Work to Do”, *3 Eur. Data Prot. L. Rev.* (152:17)

Norris, C. et al, (2017) *The Unaccountable State of Surveillance* [ebook] Springer International Publishing

Olsson, M. (2015) *JavaScript Quick Syntax Reference*, 1st edn, New York: Springer Science+Business Media

Olsson, M. (2016) *PHP 7 Quick Scripting Reference*, 2nd edn, New York: Springer Science+Business Media

O'Neil, C. (2016), *Weapons of math destruction: how big data increases inequality and threatens democracy, 1st edition*, New York: Crown, pp. 68-83

Pomerantz, J. (2015) *Metadata,* 1st edn, Cambridge: MIT Press

Rabinovich, P. (2013), "Secure cross-domain cookies for HTTP", *Journal of Internet Services and Applications* (4:13).

Ristic, I. (2005). *Apache Securit*y. O'Reilly Media. p. 280

Schoen, S. (2009), "New cookies technologies: Harder to see and remove, widely used to track you" *Electronic Frountier Foundation* [Online]. Available at: https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide

(accessed: 10th June 2018)

Schwartz, J. (2001) "Giving Web a Memory Cost Its Users Privacy", The New York Times, 04 september [online]. Available at: https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html (accessed: 10th June 2018)

Schweighofer, E. et al. (2017) *Privacy Technologies and Policy*, 5th Annual Privacy Forum, APF, pp. 185-188

Seyyar, M. S., Çatak, F. Ö., Gül, E. (2017), “Detection of attack-targeted scans from the Apache HTTP Server access logs”, *Applied Computing and Informatics* (14:18), pp. 28–29

Singel, R. (2010) “Online Tracking Firm Settles Suit Over Undeletable Cookies” *Wired*, 12 May [online]. Available at: https://www.wired.com/2010/12/zombie-cookie-settlement/ (accessed: 1st September 2018)

Sipior J. C., Ward B. T. and Mendoza R. A. (2011) “Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons” *Journal of Internet Commerce* (10:1), Available at: 10.1080/15332861.2011.558454 (Accessed: 10th June 2018), p. 3

Sörensen, O. (2013) “Zombie-Cookies: Case Studies and Mitigation” *The 8th International Conference for Internet Technology and Secured Transactions* (ICITST-2013), pp. 321-322

Steeves, V. (2009) “Data Protection Versus Privacy: Lessons from Facebook’s Beacon”, *The contours of privacy*, ed. Matheson D., 1st edn, Newcastle upon Tyne: Cambridge Scholars Publishing

Tene, O. and Polonetsky, J. (2012) “To Track or ‘Do Not Track’: Advancing Transparency and Individual Control in Online Behavioral Advertising” *Minnesota Journal of Law, Science & Technology* (13.1), pp. 245-249

Trevisan, M. et al. (2017) “Uncovering the Flop of the EU Cookie Law” [online]. Available at: https://arxiv.org/pdf/1705.08884.pdf (accessed: 14th June 2018)

Turban, E. et al. (2017), *Introduction to Electronic Commerce and Social Commerce*, 4th edn, [ebook] Springer Texts in Business and Economics, pp. 14-16

Ustaran, E. (2018) *European Data Protection: Law and Practice*, 1st edn [ebook] IAPP, pp. 154-155

Utz, C. et al (2018) "We Value Your Privacy...Now Take Some Cookies: Measuring the GDPR’s Impact on Web Privacy", [online]. Available at: https://arxiv.org/pdf/1808.05096.pdf (accessed: 18th June 2018), p. 8

Voigt, P. and von dem Bussche, A. (2017) *The EU General Data Protection Regulation (GDPR) Practical Guide* [ebook] Springer International Publishing, p. 11

Yue, C., Xie, M., and Wang, H. (2007) "Automatic Cookie Usage Setting with CookiePicker", *IEEE DSN 2007*, Edinburgh: UK, June.

Zuiderveen Borgesius, F. and Poort, J. (2017) *Online Price Discrimination and EU Data Privacy Law*, J Consum Policy [online]. Available at: https://ssrn.com/abstract=3009188

LEGAL INSTRUMENTS

Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994)

Council of Europe (1950), *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, available at: http://www.refworld.org/docid/3ae6b3b04.html (Accessed: 17th June 2018)

Council of Europe (1981), *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. European Treaty Series - No. 108. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37 (Accessed: 17th June 2018)

Commission Proposal (2016), *Proposed Code of Conduct on privacy for mobile health applications*, available at: https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised (accessed: 11th June 2018).

Commission Proposal (2017a) *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, 10.1.2017 COM(2017) 10 final 2017/0003(COD). Availabe at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010&from=CS (Accessed: 17th June 2018)

Commission Proposal (2017b) *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a framework for the free flow of non-personal data in the European Union*, COM/2017/0495 final - 2017/0228 (COD), Brussels: s.n.

Council Proposal April (2018), available at: https://iapp.org/media/pdf/resource_center/ePR_2018-04-13.pdf (Accessed: 26th June 2018)

Council Proposal March (2018), available at: https://iapp.org/media/pdf/resource_center/ePriv-reg_03-2018.pdf (Accessed: 26th June 2018)

Council Proposal May (2018), available at: https://iapp.org/media/pdf/resource_center/Draft-ePriv-Reg-May-2018.pdf (Accessed: 26th June 2018)

Council Proposal July (2018), available at: https://iapp.org/media/pdf/resource_center/ePR-draft-July-2018.pdf (Accessed: 26th June 2018)

Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU Text with EEA relevance, OJ L 173, 12.6.2014, p. 349–496, Brussels: s.n.

EDPS Opinion 05/2018 (2018) on privacy by default and by design, available at: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (accessed: 18th August 2018)

EDPB Statemente (2018), *Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications.* Available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf (Accessed: 26th June 2018)

ENISA (2012), *Privacy considerations of online behavioural tracking* [Online]. Available at: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking (Accessed: 10th June 2018), p. 11.

European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02, available at: http://www.refworld.org/docid/3ae6b3b70.html (Accessed: 7th June 2018)

European Union, *Consolidated version of the Treaty on the Functioning of the European Union*, 13 December 2007, 2008/C 115/01, available at: http://www.refworld.org/docid/4b17a07e2.html (accessed: 11th June 2018)

ICC UK (2012) "Cookie guide", 2nd edn [Online] Available at: https://www.cookielaw.org/media/1096/icc_uk_cookiesguide_revnov.pdf (Accessed: 10th June 2018)

Mid-Term Review of Digital Single Market Strategy for Europe (2017) [online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1496330315823&uri=CELEX:52017DC0228 (accessed: 19th June 2018)

The European Parliament and the Council of the European Union, 1995. *Directive 95/46/EC of the European Parliament and 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*, s.l.: s.n.

The European Parliament and of the Council of the European Union, 2002. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the 58processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, Brussels: s.n.

The European Parliament and the Council of the European Union, 2016. *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, s.l.: s.n.

UN General *Assembly, Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), available at: http://www.refworld.org/docid/3ae6b3712c.html (Accessed: 17th June 2018)

UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available at: http://www.refworld.org/docid/3ae6b3aa0.html (Accessed: 17th June 2018)

Working Party Guidelines (2017) *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=47742 (accessed: 14th June 2018)

Working Party Opinion 04/2012 (2012) *on Cookie Consent Exemption*

Working Party Opinion 02/2013 (2013) *providing guidance on obtaining consent for cookies*

Working Party Opinion 06/2014 (2014) *on the notion of legitimate interests of the data controller*

CASE LAW

In re DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001)

Lane v. Facebook Inc. Nos. 10–16380, 10–16398.

SSHD v Tom Watson & Others C-698/15

Tele2 Sverige AB v Post-och telestyrelsen C-203/15

Wirtschaftsakademie Schleswig-Holstein GmbH v. Facebook Ireland Ltd, C-210/16 of June 5th 2018

COOKIE POLICIES

Alphabet, 2018, *Cookie Policy*. [Online] Available at; https://www.alphabet.com/en-gb/alphabet-cookie-policy (Accessed: 28th August 2018)

Amazon, 2018a, *Cookie*. [Online] Available at: https://www.amazon.co.uk/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=201890250 (Accessed: 28th August 2018)

Amazon (2018b) “Third Party Cookies” [online]. Available at: “https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=GDDFZHDDGWM46YS3&pop-up=1 (Accessed: 28th August 2018)

Facebook, 2018. *Cookie*. [Online] Available at: https://www.facebook.com/policy/cookies (Accessed: 28th August 2018).

Google, 2018, *Cookie Policy*. [Online] Available at: https://policies.google.com/technologies/cookies?hl=en (Accessed: 28th August 2018)

ICANN, 2018, *Cookie*. [Online]. Available at: https://www.icann.org/privacy/cookies (Accessed: 12th July 2018)

Instagram, 2018, *Cookie Policy*. [Online] Available at: https://help.instagram.com/1896641480634370?ref=ig (Accessed: 28th August 2018)

Twitter, 2018, *Cookie Policy*. [Online] Available at: https://help.twitter.com/en/rules-and-policies/twitter-cookies (Accessed: 28th August 2018)

WhatsApp, 2018, *Cookie*. [Online] Available at: https://www.whatsapp.com/legal/#cookies (Accessed: 28th August 2018)

Wikimedia, 2018, *Cookie Statement* [Online] Available at: https://foundation.wikimedia.org/wiki/Cookie_statement (Accessed: 28th August 2018)

OTHERS

Bird & Bird (2018) “Penalties” [Online] Available at: https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/penalties (accessed: 10th Augst 2018)

Catb.org (2003) "Magic Cookie", [online]. Available at: http://catb.org/jargon/html/M/magic-cookie.html (Accessed: 10th June 2018)

Cookielaw.org (2018) "Google Analytics EU Cookie Law", [online]. Available at: https://www.cookielaw.org/google-analytics-eu-cookie-law/ (accessed: 10th June 2018)

Council of Europe (2018) “Chart of signatures and ratifications of Treaty 108” [Online] Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=FzU9953g (accessed: 10th June 2018)

DLA Piper (2016) “EU Law on cookie”, [online]. Available at: https://www.dlapiper.com/~/media/Files/Other/EU_Cookies_Update.pdf (accessed: 2nd July 2018)

European Commission (2017) "Cookie" [online]. Available at: http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm (accessed: 1st September 2018)

Flash Eurobarometer 433 (2016), “E-Privacy Report” [online]. Available at: http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/FLASH/surveyKy/2124 (accessed: 9th July 2018)

Garante della Privacy (2014) “Individuazione delle modalità semplificate per l’informativa e l’acquisizione del consenso per l’uso dei cookie” [online]. Available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3118884 (accessed: 7th July 2018)

Glossary of the EDPS (2018), “Data Minimisation” [online]. Available at: https://edps.europa.eu/node/3099#data_minimization (accessed: 29th July 2018)

|Nu.nl (2018), “NPO krijgt boete van 25.000 euro voor cookiebeleid”, 16 September [online]. Available at: https://www.nu.nl/internet/3954459/npo-krijgt-boete-van-25000-euro-cookiebeleid.html (accessed: 16th September 2018)

Publicsuffix.org (2018), “Public Suffix List” [Online] Available at: https://publicsuffix.org/list/public_suffix_list.dat (accessed: 10th June 2018)