

Cookies and the protection of personal data under the GDPR

ملفات تعريف الارتباط (الكوكيز) وحماية المعطيات الشخصية في إطار

التنظيم الأوروبي لحماية المعطيات الشخصية (GDPR)

Dahmani Samir

Mouloud Mammeri University of Tizi-Ouzou.

Faculty of Law and Political Science

samir.dahmani@ummto.dz

Date of submission:16/10/2025 Date of final acceptance:14/12/2025 Date of publication :December 2025

Abstract:

Cookie Tracking allows website owners to collect and store huge amounts of information about users during a connection to a website, in order to make it easier to browse and to track the behavior of each user in a very precise way. In fact, this information contains personal data including the IP or email address, first and last name, images, geographical data of the visitor (GPS), or even his behavior on the visited website (devices, links, web pages consulted, etc.), which may be used by third parties, which could pose a security risk.

However, these practices are currently strictly regulated by the GDPR, which oversees all collection and processing of personal data from individuals within the EU.

Keywords: Personal data; Third-party cookies; Profiling; Treat; GDPR.

ملخص:

تُتيح ملفات تعريف الارتباط (الكوكيز) لأصحاب مواقع الإنترنت، عملية جمع وحفظ معلومات هائلة عن المستخدمين أثناء دخولهم إلى هذه المواقع الإلكترونية، حيث تقوم هذه الملفات بتسهيل عملية التصفح وتُتبع سلوك كل مستخدم بدقة عالية، إذ أنّ هذه المعلومات تحتوي في الواقع على بيانات شخصية للمستخدمين على غرار : عنوان التعريف (IP) أو البريد الإلكتروني، الاسم واللقب، الصور، بيانات الموقع الجغرافي للمستخدم (GPS)، وحتى سلوك المستخدم في موقع الويب الذي زارهُ (باستخدام الأجهزة، والروابط، وصفحات الويب التي تم الوصول إليها، وما إلى ذلك)، والتي قد يتم استغلالها من طرف الغير وما يُصاحبها من مخاطر أمنية.

إنّ هذه الممارسات حالياً قد تم تنظيمها في إطار التنظيم الأوروبي المتعلق بحماية المعطيات ذات الطابع الشخصي (GDPR)، الذي نظم جميع العمليات المتعلقة بجمع ومعالجة وتحويل البيانات الشخصية في إطار الاتحاد الأوروبي.

الكلمات المفتاحية: البيانات الشخصية؛ ملفات التعريف للغير؛ التنميط؛ المعالجة؛ (ت.ع.ح.ب).

Auteur correspondant : Dahmani Samir

Introduction :

The digital revolution has given rise to many technologies that have been developed and used by the operators of digital platforms, in order to offer a better quality service to the Internet user, and then identify and observe his browsing behavior on the same site, using the technology of cookies that automatically generate personal data without the knowledge of customers, since the collection and management of this data represent for e-commerce sites, the heart of the marketing system, their activity and their development.

The owners of the e-commerce sites use the providers of web tracking technology, with the aim of helping them to better profile visitors, and to target advertising or exploit the data collected for commercial purposes, but the processing of these data has become commonplace for some economic actors of the web.

E-commerce sites rely on cookies to analyze consumer behavior and its impact on sales, as well as to identify pages previously visited by consumers. These data provide them with information that can guide the decision of potential customers and distinguish their online distribution service from that of their rivals.

Personal information collected through third-party cookies becomes an essential resource for operators of digital platforms, such as Facebook, Beacon, Google AdSense, AdBrite, Yahoo, Twitter and others. Such data enable them to offer specific services whose value depends on the creation of data by the users themselves, but also to generate advertising revenue that finances the production of informational goods and online services that are often offered for free. We then see an increase in the amount of personal data unintentionally disclosed by users in exchange not only for content, but also for services they had not previously used.

The methods used by websites for the illegal collection of surfing data of Internet users, via harmful cookies and other tracking techniques (web tracking), have led to a considerable increase in the volume and diversity of data saved and processed without the consent of users, (such as name, address, credit card number, type of purchase, product categories and frequency of purchases, etc.), for the benefit of political parties, organizations, digital companies, associations, telecommunications operators, etc.

These practices have given rise to serious concerns about the security and safeguarding of personal data, thus becoming a real challenge for democratic states such as the European Union (EU), which has adopted a general regulation on the protection of personal data, commonly referred to as "GDPR", in order to ensure homogeneous protection of such data throughout the European Union, while guaranteeing citizens of all Member States identical and enforceable rights, as well as obligations and responsibilities for controllers and processors.

The use of personal data collected in this way by means of cookie technology mainly benefits their operators (operators of digital platforms), from whom large amounts of data are subject, in a few fractions of a second, to intra-EU, intra-EU and extra-EU commercial transactions. However, these operators exploit the programs and applications on smartphones, tablets and other devices provided by online intermediaries to illegally collect personal information from consumers.

In this context, the GDPR has fundamentally changed the provisions laid down in the former Directive 95/46/EC (Repealed) of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It calls for a redefinition of the concept of "personal data" and a rethinking of new forms of communication regulation. To do this, our approach consists in analyzing the links between cookies and personal data, as well as the strategy for collecting and using personal data adopted by the websites. This study therefore raises questions related to the subject, including: Are cookies personal data? If so, what is the purpose of the collection of this information by cookies?

What is the GDPR's position regarding the data collected and processed via cookies?

In order to address these issues, we have followed an inductive and analytical approach, through which we will first address the various concepts related to the subject (**section I**), and the typology of cookies (**section II**) and their areas of use (**section III**). Next, we will present the various disadvantages of third-party cookies (**section IV**), and cookies and the new obligations established by the GDPR (**section V**). We will then study the effects of third-party cookies on the privacy of the data subjects (**section VI**). Finally, we will conclude on the impact of the GDPR on operators of web platforms (**section VII**).

Section I: Definitions

The data generated by internet cookies can be used for various purposes by many actors worldwide.

A) The web tracking:

Web tracking is an operation that consists in tracking the evolution of visitors to a website, and knowing its itinerary and the time spent on each of the pages visited¹, but there are many web tracking techniques (Cookies, Pixel, Digital fingerprint, Kissmetrics, Google Analytics, bihaviorial, canvas fingerprinting, etc.), the simplest of which consists in recording and analyzing log files on the server of the visited website, as well as the browser transmitting information to the server on each consultation carried out, in particular relating to the operating system and the type of browser and the language of the browser, the IP address or the URL of the visited web page.

However, web tracking via cookies goes further, but more complex tracking methods have been used to record and analyze personal data in more detail, such as scrolling and the number of clicks made by the user on the website visited, as well as information that determines for example whether the user actually read an article on the website visited, and how quickly he did so?, and whether he reads comments written in response to an article, etc.².

In the context of targeted advertising, web tracking allows advertisers to target different segments of the public, and to easily measure the success of an advertising campaign, the more complete the information from web tracking, the more accurate the targeting.

Now that, the user's browsing behavior is analyzed in particular by means of third-party cookies, that is why the web tracking service provider broadcasts image files (advertising banners or pixel tags), which are integrated into the website consulted and establish the connection with the servers of the third party, on which the user will be (have) recognized by various sites and services, without him being able to notice it.

Indeed, social plugins allow website managers to use the possibility to integrate various social networking services directly on their platforms, such as the Facebook "Like" button, in order to analyze user behavior and obtain accurate statistical information, and as soon as the user goes to the website, tracking data such as the user's IP address and the address of the website visited, etc., are automatically transmitted to the Facebook provider, since the information transmitted will also include the content that he/she had liked³.

B) Cookies:

Before defining what a cookie is, it is important to emphasize that these are neither installable nor executable programs on a computer, nor malware or viruses. However, some cookies can be spotted by various antivirus programs, as they have the ability to monitor users' online actions.

In any case, 'cookies', also called 'cookies' or 'tracking cookies', are small files that enable information to be stored on web browsers, which enable the creation of data profiles that contain information relating in particular to the user's browsing preferences, the banner advertisements on which he clicks, or the length of time he has visited each web page of certain websites. Here again, the small file (the cookie) is automatically saved on the hard disk when visiting certain websites and when installing the software or a mobile application.

In some cases, cookies allow the user not to have to set these specific preferences (the language of the site, etc.) each time websites and resources are visited, because they contain a “unique identifier” similar to a label that is recognized by a website when it reads the cookie stored (stored) on that user’s device, it recognizes it and knows that it has already consulted that site, in other words, a cookie is specific to the website that deposited it, and only the site that made the deposit is the only one able to return to consult the tracker in question, nevertheless, the information contained in it is then inaccessible by the other websites.

Thus, the cookie is essentially a simple text file or information that is stored on the user's hard drive by the server of the site or service that he has visited. This text file may contain various information such as: the identification of the server that has placed the cookie, a unique identifier in the form of a number and sometimes a possible expiry date⁴.

However, cookies are stored invisibly and can have undesirable effects, because the user generally cannot know what they contain or what they trigger, and in many cases this results in an undesirable, behavior-oriented and target group-oriented advertising flow⁵.

C) Personal data:

Article 04-1 of the General Data Protection Regulation (GDPR), also known by its English acronym GDPR (General Data Protection Regulation), provides a very broad definition of personal data. This includes any information about an identified or identifiable natural person, such as surname, first name, home address, e-mail address such as “prenom.nom@entreprise.com”, identification number (such as social security, passport, etc.), internet protocol (IP) address, search history and browser (cookies, tracers, etc.), location information (GPS), health data that would allow the specific identification of a person (blood group, etc.), as well as biometric data, ethnic and racial information, sexual orientation, political beliefs, religious beliefs, or other details specific to that person⁶.

In order for data to be considered personal, the GDPR does not require that it be contained in a database or even exploitable by the person who collected or holds it, while the regulation does not specify the format of the file containing this personal data, so they can be videos (Video surveillance...), images (Photographs, painting, etc.), sounds (Audio or voice recordings), or better still a fingerprint or retina, etc.

According to Article 04/2 of the GDPR⁷, any operation carried out on personal data, whether manual or automated, such as the collection, recording, storage, modification, consultation, distribution or deletion of such personal data is considered to be a data processing operation. This includes: personnel management and salary administration, using a contact database containing personal information, sending promotional emails, posting or displaying a photo of an individual on a website, collecting IP addresses, storing video surveillance captured via cameras, drones or satellites, etc.

With this definition, the Regulation (GDPR) has strengthened and deepened the concept of ‘personal data’, and addressed the shortcomings of Directive 95/46/EC, which is repealed with effect from May 25, 2018.

Section II: Cookie typology

Cookies have been designed as a service to provide websites with memory capacity, allowing users to be offered personalized recommendations based on their interests and needs. These cookies can be classified in one of the following categories according to their origin (A), duration (B) and usefulness (C).

A) The function of cookies according to their origin

1- Proprietary cookies: These are cookies that ensure the proper functioning of the website that the user consults. They serve to store and preserve information relating to the user during his navigation, but also during his successive visits, thus facilitating his navigation on a website⁸.

2- Third-party cookies: These cookies are installed by third parties on the site that the user has already visited, with the aim of collecting data to better understand his behavior and his desires in advertising.

In general, most browsers such as: Mozilla, Firefox, Microsoft Internet Explorer and Opera, etc., are configured to accept third-party cookies. However, it is precisely this type of cookie that causes the most concern among users. However, they have the option to change the browser settings to prohibit them. For this purpose, there is no inherent danger in the acceptance of third-party cookies that make certain web functionalities possible. However, they are also used to track users from site to site⁹.

B) cookies according to their duration

1- Session cookies: These cookies are mainly used by online shops in order to retain (cookies) the products that the buyer has added to the shopping cart during a single buying session. In other words, these cookies have been set to offer a method of implementing online shopping baskets, a virtual mechanism where the user can gather the products he wants to acquire while browsing the e-commerce site¹⁰.

However, applications such as shopping baskets favor storing the list of items in a database on a server rather than saving them directly in the cookie. In this context, the server transmits a cookie including a distinctive session identifier, which will subsequently be returned by the browser on each new request. Thus, the items placed in the basket are recorded and linked to this same unique session identifier.

For this purpose, the regular use of cookies is beneficial to connect to an online shopping platform via identifiers. Thus, the web server first transmits a cookie that contains a unique session identifier, then the users must enter their credentials (a user name and a password). The web application then authenticates the session, thereby allowing the user to access the service.

2- Permanent or persistent cookies: These cookies are used to store the user's personal information, such as: a username, password, contact details and account number, in order to prevent the user from entering them systematically when visiting a website, but these cookies may remain on the hard drive of the machine for a certain time after the session has ended. In addition, some cookies remain in the hard drive for life if the user does not delete them.

In any case, permanent cookies serve to identify whether a user is logged in and under which identifier (authentication), they also save the login details so that users do not have to remember their passwords on the sites. In addition, these cookies track repeated visits to the same site over time¹¹.

C) Cookies based on their usefulness

1- Advertising cookies: These cookies allow advertisers to perfect their ads and customize promotional content according to each customer's interests, by detecting their buying behavior or certain specific preferences.

2- Security cookies: These are cookies that ensure that the information contained in the cookie is encrypted when it is transmitted between the website and the browser. These cookies are only sent by a secure "https" server, which notably ensures e-commerce transactions and banking services¹².

Section III: Areas of use of cookies

It is possible that some cookies are used to store information about the user of a site, or they are aimed at other more or less avowed purposes¹³:

A) Marketing and advertising: These cookies allow online store owners to tailor their advertising according to the activities carried out on each site visited, in order to display relevant content to customers in the future. This is where they collect valuable consumer information or data, giving them the ability to identify each consumer's interests and track their journey through the site they are exploring.

These cookies (third-party cookies) allow advertisers to display more specific and targeted advertisements on their websites, with the aim of attracting and satisfying potential customers. At the same time, advertising companies are eager for the essential information or data collected by these cookies that they use to adapt the messages and advertisements presented to consumers.

B) Browsing and connecting: Many websites use cookies to facilitate the user's navigation on their platform, by saving their preferences (language, geographical position, etc.), as well as the articles or content they have consulted.

C) Statistics and profiling: Tracking cookies are used to observe users' online behavior, while tracking on the same site is generally intended for statistical purposes (number of pages viewed, location of visitors, routes, etc.). For example, advertisers use third-party cookie tracking on various sites to establish anonymous user profiles, with the objective of defining which advertisements should be presented to the user and, if their email address is available, to send them emails in connection with these promotions¹⁴.

Section IV: The disadvantages of third-party cookies

The use of third-party cookies poses a major challenge for data protection and for law enforcement authorities. Unfortunately, the personal data collected and disseminated by these cookies have become merchant products, items that can be bought, sold and exchanged. Moreover, these data flows occur across borders. This poses significant privacy risks due to unequal data protection laws in third countries, or even the fact that many data controllers or recipients are not bound by data protection standards.

Indeed, many websites integrate information from various origins. Each site has several types of third-party cookies that are configured on the user's browser, from other platforms operating the web (Google, Facebook, Yahoo!, Amazon, Snapchat, Pinterest, Twitter, Instagram, etc.). This implies that the site manager uses plugins belonging to these operators such as Google Tag Manager or a comments section on one of the Facebook pages, among others.

Thus, in the field of digital marketing, companies use a powerful artificial intelligence management tool (Hootsuite, Digimind, Tweetdeck, Radarly, etc.), which uses and manages multiple social media accounts, and allows users to write and read messages simultaneously, without the account holders knowing who is collecting or intercepting information about them (third-party cookies or other computer cookies)¹⁵.

In other words, Google's standard third-party cookies, for example, generate separate identifiers for each user in order to track them on all other web platforms. Cookie IDs, which frequently track users online, can be used to create detailed anonymous profiles of people. These profiles could subsequently be sold to digital advertising agencies or exploited for behavioral-based marketing, or even used for malicious purposes¹⁶.

In fact, third-party cookies are not created by a specific website, but are generated by one of the objects or images on the page that come from another website. In other words, the images and other elements present on a web page can be hosted on servers separate from the one that hosts this page, and to display the latter, the browser must download all these elements and images accordingly¹⁷.

For example, when I enter the URL (www.amazon.com) in my browser, it often happens that items such as images or advertisements, or other components on the page come from a website other than (www.amazon.com). This also includes cookies from unsolicited pop-ups.

Generally, a website should not have the ability to create or modify cookies associated with another site. However, a breach of security in a browser can offer harmful sites the opportunity to violate this rule, exploiting a vulnerability typically referred to as "cross-site cooking", with the aim of manipulating the browser's recent cookies or stealing the session identifier, among other things. For this reason, Internet users are advised to opt for the most current versions of browsers, where these flaws are almost completely fixed or removed¹⁸.

However, many e-commerce sites use third-party cookies to track users across all web pages visited. This includes the location of advertising images or a surveillance pixel, as well as most personalized ads and spam-labeled junk emails. They come from the information collected by tracking cookies.

This is why web users are suspicious of third-party cookies, as they pose a threat to their privacy. Indeed, any website, regardless of its size or dynamic system, can potentially house dozens of trackers and Trojan horses that collect users' personal data without their knowledge and permission¹⁹.

In this respect, hackers use sniffer software that penetrates the computer systems of Internet users, in order to capture and record data relating to the visits made by these Internet users, such as the number of people connected, the date and time of connection, the address on the Internet, the protocol of the computer, the web pages consulted, as well as the analysis of the cookies of the connected computer, etc., however this information makes it possible both to detect possible computer intrusions and to estimate the number of visitors to the site visited, which are, most often, carried out daily, in particular by the host of the site²⁰.

Section V : Cookies and the new obligations established by the (GDPR)

In an era of globalized transactions, the management of personal data through cookies knows no limits and online tracking technologies increasingly facilitate the collection and storage of information without the knowledge of the user, without the knowledge of who collects or intercepts his information, and to counter these practices as well as the risks associated with cross-border data flows, the European legislator has introduced new rules governing the sharing of personal data (A), which all web actors handling this information must respect in accordance with the GDPR (B).

A) What does the Cookie Regulation (GDPR) say?

It is important to know that tracking technologies are constantly evolving, which makes the term “cookies” very broad, since it includes all the different tracers deposited or read. These can be used when consulting emails, when visiting a website, or when using a software or application. However, these cookie files may contain texts and personal information disclosed by the user during his navigation, such as his name, his date of birth, his address, his profession and other types of information related to the data subject²¹.

Generally, cookies contain an identifier known as a (Cookie ID) considered personal information according to the (GDPR). This identifier fits perfectly into the definition given in Article (04) concerning online identifiers, as a direct or indirect reference to an individual. For this purpose, when a cookie identifier is established on a user's browser, it is integrated into the majority of cookies. Each user benefits from a distinct identifier that allows websites to remember that specific user and his references and his settings when he returns to the site he has previously visited.

From now on, all regulation concerning personal data also applies to cookies. This means that the General Data Protection Regulation (GDPR) applies regardless of the device used to collect and process personal data. This includes computers, smartphones, tablets, drones, applications (such as video game consoles connected to the Internet), smart watches and even connected cars, etc.²².

In all circumstances, the General Data Protection Regulation (GDPR) is applicable to all personal data processing operations carried out by companies or their subcontractors located in the EU, as well as outside the EU when they aim to offer goods and/or services to EU residents. This also includes monitoring user behavior as long as it takes place within the EU²³.

In short, all companies and their subcontractors that collect and process personal data belonging to EU citizens are obliged to comply with this Regulation (GDPR), and to guarantee the highest level of protection of such data upstream, regardless of where the processing takes place²⁴.

B) Compliance of websites with the obligations of the (GDPR) :

Personal data in the EU (European Union) is protected by the (GDPR), which sets new requirements that will have to be taken into account, but the website owner must absolutely respect the principles concerning the lawfulness of the processing of personal data, as defined by Articles (05) and (06) of the (GDPR), and provide visitors to his website with the information cited thus in Articles (13) and (14) of the (GDPR)²⁵, in which it must provide clear information about the data collected, as well as about the purpose of cookies, and block access to cookies until visitors have given their explicit consent for a specific use. In addition, it is necessary to offer them the possibility to accept or refuse cookies, and to withdraw their consent at any time. He must also request the renewal of this consent at least once every twelve (12) months. In addition, the website must securely keep a complete document as legal evidence, including all consents granted. In any case, it is imperative that he obtain the prior consent of the individuals concerned before the implementation of cookies. In addition, it must inform them about the purposes of these cookies and offer them a possibility to oppose them²⁶.

However, the acceptance of cookies remains a central element of website compliance for EU-based users. In addition, a website based outside the EU must comply with GDPR standards if it collects personal information from users in the EU. Thus, the authorization concerning cookies is now the legal basis generally used, allowing websites to manage and exploit personal data via cookies²⁷.

Under the (GDPR), explicit and prior consent must be obtained before any activation of cookies, except for cookies that are essential for the proper functioning of an online service, such as cookies related to the electronic shopping cart (E-shop), authentication settings (Security of E-banking services), choice of language or browser, etc., moreover, third-party cookies will not be necessary, that is to say they will not be exempted by the (GDPR), but the user site of these cookies will have to obtain the prior and explicit consent of the data subjects before this website is allowed to activate them.

Therefore, consent must be granted freely (without constraint or in exchange for service) and in a granular manner, that is to say, users must have the possibility to enable some cookies rather than others, without being constrained to all or none²⁸.

On most websites, the required information regarding the use of cookies will be presented in the form of pop-up windows or cookie banners, also known as warning banners. This is because there are various plugins dedicated to this task, such as Cookie Notice, Cookie Law Info or EU Cookie Law. In this situation, the user has the possibility to consent or refuse cookies individually, for each site, by clicking on the banner that must be displayed on his first visit to the website.

However, the cookie banner on a website is not allowed to pre-check boxes, and the use of internet users' data cannot be interpreted as valid consent. In fact, they must expressly and positively express their agreement to allow the activation of cookies and the processing of their personal data.

For this purpose, the cookie banner developed and offered by Cookiebot or Cookiesecure technology, etc., meets the requirements of personal data protection, and that in the absence of choice no tracer is put in place, however these banners have grouped cookies into four (04) purpose categories: necessary, preferences, statistics and marketing, to which only cookies strictly necessary for the basic functioning of the website are checked by default.

On the other hand, all other cookies and similar trackers are automatically detected and blocked by a high-performance scanner, until the user's consent is obtained, which will be automatically and anonymously recorded and stored using an encrypted key for a specified period of time. In France, for example, the (Cnil) recommends that cookies have a maximum duration of 13 months, which can be extended on a new visit if the banner reappears. However, some cookies can persist much longer, such as those from Google Adwords which can last up to 540 days. There are even cookies designed to last more than 7000 years²⁹.

In this respect, the question of the retention period of personal information (that which can identify a natural person, directly or indirectly) has become particularly sensitive. To this end, the

(GDPR) does not set a specified period for the retention of such data, but it does emphasize the principle of limitation of retention in Article (5.1.e)³⁰, which prohibits their retention for a longer period than deemed necessary in view of the purposes for which they are processed, this means that, the duration of retention of the data must be determined by the controller taking into account the purpose for which they were collected³¹.

Section VI: Privacy and third-party cookies

Directive 2002/58/EC of July 12, 2002 on privacy and electronic communications (**e-privacy**), which was amended by Directive 2009/136/EC of November 25, 2009, contains, inter alia, provisions on the use of cookies, and the processing of traffic and location data, access to stored data, confidentiality of communications, etc. According to Article (5/3) of this Directive, it is allowed to store data (such as cookies) or to access this data stored in the terminal of the subscriber or user only if the subscriber or user is clearly and fully informed of the purposes of the processing. In addition, the user must have the possibility to object to the processing carried out by the data controller (in accordance with Directive 95/46/EC). However, this Article (5/3) also specifies that the storage of data for technical reasons is exempted from this regulation³².

Furthermore, cookies have been fueling debates on privacy, especially since the entry into force of (GDPR), which replaced Directive 95/46(repealed) from May 25, 2018 and the disagreement between EU states on sensitive issues of future European regulation (e-privacy) would imply its adoption, as Member States have so far been unable to agree on a compromise accepted by the Parliament and the European Commission, i.e. between those who are afraid of losing their prerogatives, and those who fear a decrease in the level of privacy protection, and those who, on the other hand, consider that too many rules are imposed. In short, the compromise seems difficult on the adoption of a new text (e-privacy)³³.

Indeed, the EU General Data Protection Regulation (GDPR) is often seen as one of the most important and influential pieces of legislation on the protection of personal data, but the absence of a new regulation (e-privacy) allows EU Member States to retain the provisions of the current Directive (Directive 2002/58/EC of July 12, 2002 (e-privacy), as amended by Directive 2009/136/EC of November 25, 2009), which gives them greater flexibility³⁴.

Section VII: The impact of the (GDPR) on operators of web platforms

The European General Data Protection Regulation (GDPR) has recently introduced a contemporary perspective in response to data protection challenges. This strengthens the rights of the individuals concerned, giving them greater control over the methods used to collect and process their data. Thus, it imposes a set of obligations on web actors to assume responsibility for the protection of personal data³⁵.

In addition, the Regulation (GDPR) requires online platform operators to prove compliance through data protection principles. This requires the adoption and establishment of appropriate policies and procedures based on the potential risks related to the protection of personal data. There is also a need to manage the principles of transparency and accountability, as well as the rights of data subjects, while establishing an appropriate framework for compliance and an organizational culture focused on data security and confidentiality. This allows operators to avoid heavy penalties that would be imposed by the independent supervisory authorities in each EU Member State, which are responsible for enforcing the GDPR³⁶.

Moreover, more than (70) fines have already been imposed on companies in Europe for non-compliance with the (GDPR), and European regulators have distributed between may 25, 2018 (the entry into force of the GDPR) and January 27, 2020, more than (114) million Euros in fines and received no less (160 000) notifications for violation of the (GDPR) Regulation, yet France is now

the country that has granted the largest fine (50 million Euros) to a company, Germany and Austria imposed fines of EUR (24.5) million and EUR (18) million respectively³⁷.

In this context, the French Council of State on January 21, 2019 approved the severe penalty imposed by the CNIL (Commission Nationale de l'Informatique et des Libertés) on the American company Google, amounting to EUR (50) million³⁸, for a consent collected in a non-compliant manner in the context of advertising targeting, since the company (Google) had disregarded the provisions set out in Articles (12) and (13) of the (GDPR), relating to the right to information of persons concerned by certain data, as well as the terms of their consent to the processing of these data laid down in Articles 04-11 and 06, 07 of the said Regulation (GDPR)

The Council of State analyzed these provisions on the basis of the judgment 'Planet 49', delivered by the Court of Justice of the European Union (CJEU) on October 1, 2019³⁹ in which it 'Conseil d'État' recalls that free, specific, informed and unambiguous consent must be express, provided in full knowledge of the facts and after adequate information on the use to be made of the personal data of the person concerned. Consent by means of a box ticked by default does not result from a 'clear positive act', whereas consent obtained in the context of the overall acceptance of general conditions of use of a service cannot be classified as 'specific'.

Following the adoption of the GDPR, the French Data Protection Authority (Cnil), as part of its action plan on advertising targeting, issued directives on cookies and other tracers on July 4, 2019 to specify the applicable rules and best practices to be respected. Thus, the Council of State issued a decision on June 19, 2020 following an action for annulment brought by associations and trade unions of online advertising, e-commerce and the media, in which it 'Council of State' approved, inter alia, the measures relating to the collection of consent from internet users for cookies and other tracers. Furthermore, the Council of State annulled the rule strictly and without exception prohibiting the practice of 'cookie walls', which consists in restricting access to a website if the user refuses to accept cookies and other connection tracers⁴⁰, and consequently, the Council takes note of this decision in a statement published the same day, and announces to adjust its guidelines and its future recommendation to comply with it⁴¹.

Then again, the (GDPR) establishes in its (Chapter V) the conditions governing the transfer of personal data to countries outside the EU or to international organizations. According to which such a transfer can only take place if the receiving country guarantees an appropriate level of protection for such data, as the EU Commission can determine, according to article 45 of the (GDPR), whether a third country offers an adequate level of protection due to its domestic legislation, or its international commitments.

However, without such an adequacy decision, such a transfer is not possible unless the EU-based personal data exporter puts in place appropriate safeguards that could include standard data protection clauses (SCCs) adopted by the Commission (**Art. 46 of the GDPR**) or that exporter has adopted binding corporate rules (BCRs) approved by the European Data Protection Board (EDPB) under the conditions cited in **Article 47 of the GDPR**. In the absence of these conditions, transfers are prohibited, except for a few specific derogations provided for in Article 49 of the GDPR, and a data transfer impact assessment (DTIA) must be carried out in accordance with the provisions of Article 35 of the GDPR.

On July 16, 2020, the Court of Justice of the EU (CJEU) issued a decision⁴² invalidating Decision (EU) 2016/1250 on the adequacy of the Privacy Shield agreement, also known as **the EU-US Privacy Shield**⁴³, which allows the transfer of personal data between the EU and the US, due to concerns about US surveillance programs that put the protection of such data at risk, as this agreement could allow violations of the fundamental rights of citizens of the EU and the US. The EU, whose data is transmitted by digital giants such as Amazon, Google, Facebook, among others, to the US, this could be used to monitor users' online behavior or location. Moreover, this data could be used for public security, defense and national security purposes by the US authorities (NSA, FBI, CIA, etc.), who would have easy access (espionage) within the framework of US information collection programs, without any restriction on the use of this information.

However, the (CJEU) found that the examination of Commission Decision 2010/87 concerning standard contractual clauses for the transfer of personal data to subcontractors located in third countries, in the light of the EU Charter of Fundamental Rights ‘Charter’, does not reveal any elements that could undermine its validity. To this end, it (Decision n° 2010/87) contains effective mechanisms to ensure that the level of protection required by EU law is respected and that transfers of personal data based on such clauses can be suspended or prohibited in the event of a breach of or failure to comply with such clauses⁴⁴.

This judgment is delivered by the (CJEU) following a complaint lodged with the Irish supervisory authority by Austrian national Maximillian Schrems, a user of Facebook in particular since 2008 as for other users residing in the EU, so he was a privacy activist, but opponents of Privacy Shield are particularly concerned about the spying of data when it is transferred to the United States by US security services, like the NSA and the FBI, without any limitation and without any control or possible means of redress⁴⁵.

It should be noted that the (CJEU) had already delivered a judgment on September 6, 2015⁴⁶ invalidating Decision 2000/520/EC of July 26, 2000, on the adequacy of the protection afforded by the Safe Harbor Agreement or Safe Harbor Principles, negotiated by the United States Department of Commerce with the European Commission, which allows the transfer of personal data from the EU to the USA, this means that Decision 2000/520/EC⁴⁷ asserts that the transfer of personal data from Europe to the US is possible, as the US has sufficient guarantees for the protection of privacy.

Moreover, opponents of “Safe Harbor,” including Max Schrems, who had brought several complaints against Facebook, argued that Edward Snowden’s revelations in 2013 about NSA surveillance programs showed that Europeans’ personal data were not, in fact, protected when stored in the United States⁴⁸.

In fact, US surveillance laws, such as the Foreign Intelligence Surveillance Act (FISA) 702 and the Cloud Act, allow authorities to access information stored by US-based companies, even if the data belongs to European citizens. This option is in direct contradiction with the principles of the GDPR and fuels criticism regarding the lack of protection offered by previous transfer agreements (Safe Harbor in 2015 and Privacy Shield in 2020). It is for this reason that the Court of Justice of the European Union (CJEU) has invalidated these transfer agreements⁴⁹.

Despite this, on July 10, 2023, the European Commission adopted a third agreement, the ***Transatlantic Data Privacy Framework (DPF)***⁵⁰, judging that the protective measures in the United States were now adequate. If this agreement faces significant uncertainties, it could also be called into question, notably as a result of a future judgment by the Court of Justice of the European Union (CJEU) or due to political changes in the United States.

Conclusion :

Cookies are therefore part of the technologies offered by web tracking, allowing companies (startups, SMEs, PMIs, large companies) to set up systematic collection and storage of the browsing data of all visitors on their websites. these data may include: the origin of the visitor (search engines, advertisements, links inserted in an email, etc.), the pages successively visited, the time spent on each of these pages, the links clicked by the user, etc., however these behavioral data are useful for understanding the uses, and allow via predictive analysis to anticipate the needs and better organize the merchandising (all techniques ensuring the best commercial dissemination of products) in order to generate revenue.

However, third-party cookies used by advertisers that are placed on different types of sensors or connected objects, such as, mobile applications (smartphones), search engines, social networks, connected bracelets, connected T-shirts, smart glasses, connected soles, connected headsets, smart watches and even connected cars with machine learning systems etc., allow the collection of a huge amount of personal data without the knowledge of users, to the detriment of their privacy - to the benefit of the administration, health organizations, telecommunications operators, insurance companies, banks, political parties and big retailers and businesses services, while third-party

cookies have now become commonplace for some web economic actors, as they are in the data protection viewfinder.

As a result, almost all websites use cookies as they facilitate the collection of information and make web browsing much smoother, and it would be difficult for website owners to do without them, but these cookies, in particular third-party cookies, generate debates about the protection of privacy of individuals. This comes in the context of the future European regulation (e-Privacy) and the GDPR which was implemented on 25 May 2018, set new requirements that will have to be taken into account, which companies must ensure better protection of this data, and implement the obligation to process it fairly and lawfully, for a specific and legitimate purpose.

Although the General Data Protection Regulation (GDPR) only mentions cookies once, the agreement on the use of cookies remains an essential element of the compliance of websites intended for EU users. Indeed, the GDPR stipulates that a website should only collect users' personal data after having obtained their explicit consent for a specific purpose. This is usually done on websites via cookie banners that give users the option to choose and allow the activation of some cookies rather than others when visiting a site.

Finally, it follows from that study that the GDPR requires companies to demonstrate compliance with the GDPR principles, taking a risk-based approach to the protection of users' personal data, and to implement appropriate policies and procedures to manage the principles of transparency and accountability, as well as the rights of data subjects, while establishing an organizational culture focused on data security and confidentiality, given that a good compliance framework with the GDPR requirements would enable companies to avoid heavy fines and damage to their reputations.

In addition, the ePrivacy Directive and the GDPR collectively shape the landscape of cookie consent practices, setting strict requirements for businesses operating in the digital domain. While the ePrivacy Regulation awaits its finalization, it is clear that the regulations governing cookies and user consent continue to evolve in response to technological advances and emerging privacy concerns.

In light of these findings, our study suggests that it is essential for web platform operators to remain vigilant, stay informed about regulatory updates, and take proactive measures to ensure compliance, while providing a seamless and privacy-friendly online experience for users.

¹ **Gabriel Dabi- SCHWEBEL**, « Tracker et tracking : définition (appliquées au web) », article published [online] on November 14, 2024. <https://www.1min30.com/dictionnaire-du-web/tracker-et-tracking/> (accessed on March 20, 2025.)

Peter TRUDEAU, « Qu'est-ce que le Web Tracking ? Et les trackers dans les navigateurs ? », article published [online] on May 24, 2020. <https://windowsastuce.com/> (accessed on July 12, 2025.)

² **Imane FOUAD**. "Detection and measurement of web tracking." Doctoral thesis in Informatics, Center Inria d'Université Côte d'Azur, June 29, 2021. pp. 12-15. Published [online] on December 07, 2021 on the website : HAL Id: tel-03278529 et <https://theses.hal.science/tel-03278529v2> Submitted on 7 Dec 2021 (consulted on August 02, 2025.)

For more information, please see the **FDPIC's document** (The Swiss Federal Data Protection and Information Commissioner), on: « Explications concernant le webtracking », August 2013, pp. 02, 03. Available from: https://www.edoeb.admin.ch/content/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/explication-le-webtracking-.html/pdf (consulted on August 25, 2025.)

³ **Alexandre SERRES**, « Problématiques de la trace à l'heure du numérique », revue Sens-Dessous, 2012/1. N° 10, pp. 91-93.

⁴ See the CNIL (Commission Nationale de l'Informatique et des Libertés de France) website : <https://www.cnil.fr> (consulted on July 03, 2025.)

⁵ **Sylvain MÉTILLE**, « les cookies en droit suisse », published [online] on February 08, 2025, on the website : <https://smetille.ch/2025/02/28/cookies-droit-suisse/> (consulted on June 10, 2025.)

⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L 119/1 of may 04, 2016.

Art. 04/1 : «For the purposes of this Regulation: 1) «personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; [...]. »

⁷ **Art. 04/2** of the (**GDPR**) : « ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; [...]. »

⁸ See also: **Google Operator document** on: “Delete, allow and manage cookies in Chrome”, published on 2025, from the following address: https://support.google.com/chrome/answer/95647?hl=en-gb&p=cpn_cookies (accessed on August 12, 2025.)

⁹ **B. BATHELOT**, « Cookies tiers », article published [online] on March 18, 2020, on the website: <https://www.definition-marketing.com/definition/cookie-tiers/> (accessed on August 02, 2025.)

¹⁰ **Grégory JEANDOT**, « Les cookies pour les nul en informatique », article published [online] on March 14, 2013 - Updated on March 20, 2013 at 17:13, from the following address: <https://www.e-marketing.fr/Theematique/data-1091/Tribune/Les-cookies-nule-informatique-229748.htm> (accessed on June 12, 2025.)

¹¹ For more information, please visit: <https://www.apprendre-php.com/tutoriel-13-les-cookies-.html> (consulted on May 19, 2025.)

¹² Ibid.

¹³ **Cookiebot** : « Cookies Internet : Que sont-ils et que font-ils ? », cookiebot.com, article published [online] on February 24, 2020. <https://www.cookiebot.com/fr/cookie-internet/> (consulted on January 12, 2025.)

¹⁴ **Art. 04/4** of the (**GDPR**) : « ‘profiling’ means 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; [...]. »

¹⁵ **Alexandre CHEN**, « Gérer les données personnelles fournies aux applications », revue I2D - Information, données & document, volume 43, n° 3/ 2017, pp. 47, 48.

¹⁶ **Arnaud JACQUES**, « Les Cookies informatiques et la sécurité », pp. 05-08, article published [online] on July 15, 2002, on the website: <https://www.securiteinfo.com/conseil/cookies/shtml> (consulted on June 04, 2025.)

¹⁷ **FDPIC report** (Federal Data Protection and Information Commissioner) on the "New developments in cookies", p. 02, published [online] at: <https://www.edoeb.admin.ch/content/edoeb/fr/home/documentation/rapports-d-activites/anciensrapports/18eme-rapport-d-activites-2010-2011/nouvelle-evolution-des-cookies.pdf> (accessed on June 25, 2025.)

¹⁸ **Jean-LUC MARINI**, « Le tracking est-il dangereux ? », article published [online] on March 08, 2016 at 11:00 from the following address: <https://www.journaldunet.com/ebusiness/crm-marketing/117524/> (consulted on August 21, 2025.)

¹⁹ **Gary DAGORN**, « Cookies, mouchards: comment vous êtes suivis sur internet », article published [online] on 30/03/2018 at 15:24- Updated on 14/10/2019 at 11:33, from the following address: <https://www.lemonde.fr/les-decodeurs/article/2018/03/30/> (consulted June 20, 2025.)

²⁰ **Éric ANDRIEU**, « Internet et la protection des données personnelles », revue LEGICOM, Jun 2000/1 n° 21-22, pp. 163-165. DOI: 10.3917/legi.021.0155

²¹ **Ludwig HERVÉ**, « Décryptage : les techniques de tracking avancées et les enjeux de la protection des données », article published [online] on May 16, 2017 at 09:59, updated on December 29, 2017, from the following address: <https://www.blogdumoderateur.com/tracking-enjeux-protection-donnees/> (consulted on July 09, 2025.)

²² **Valérie LAURE BENABOU**, « L'extension du domaine de la donnée », revue LIGECOM 2017/2 N° 59, pp. 06, 07. DOI: 10.3917/legi.059.0003

²³ **Art. 03 of the (GDPR)** : « 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

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

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

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

See also: the Arts. 02 and 25 of the (GDPR).

²⁴ **Catherine BARREAU**, « Le marché unique numérique et la régulation des données personnelles », revue Réalités industrielles, 2016/3 Août 2016, pp. 39,40.

²⁵ See the Arts. 05, 06, 13 and 14 of the (GDPR).

²⁶ **CNIL**: « Cookies et traceurs : comment mettre mon site web en conformité ? », published [online] on October 01, 2020, on: <https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/comment-mettre-mon-site-web-en-conformite> (accessed on June 14, 2025.)

²⁷ **Michaël TOTH**, « Consent on the web : a transdisciplinary analysis », doctoral thesis in Informaticse, Center Inria d'Université Côte d'Azur, June 19, 2023, pp. 05-08, 55-79, published on October 26, 2023, on the website: <https://theses.hal.science/tel-04259483v> (consulted on June 02, 2025.)

²⁸ **Thierry Léonard, Olivia GUERGUINOV, Etienne WERY**, « C'est quoi le consentement en matière de cookies et données personnelles ? », article published [online] on June 10, 2020, on the website: <https://www.droit-technologie.org> (accessed on July 02, 2025.)

²⁹ For more information, see the following sites: <https://www.cookiebot.com/fr/conformite-cookie-rgpd/> and <https://www.cookie-secure.com/fr/services-rgpd-dpd> and <https://www.digitalcontentnext.org/blog/2017/06/23/eus-general-data-protection-regulation-means-website-compliance/> (consulted on May 06, 2025.)

See also: La **CNIL** : « Cookies & traceurs: que dit la loi ? », published on [online] on the website: <https://www.cnil.fr/fr/cookies-traceurs-que-dit-la-loi> (accessed on June 14, 2025.)

³⁰ **Art.5.1.(e) of the (GDPR)** : «1. Personal data shall be: [...] ; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); [...]. »

³¹ For more information on this topic, consult the **CNIL**: « Les durées de conservation des données », published July 28, 2020, on the website: <https://www.cnil.fr/fr/passer-l'action/les-durees-de-conservation-des-donnees/> (consulted on August 04, 2025.)

See also: **Etienne WERY, Olivia GUERGUINOV**, « Combien de temps peut-on conserver des données personnelles ? », article published [online] on September 01, 2020, from the following address: <https://www.droit-technologie.org/actualites/> (consulted on July 12, 2024.)

³² **Directive 2002/58/EC** of the European parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O.J.E.C, L 201/37 of July 31, 2002.

Directive 2009/136/EC of the European parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, O.J.E.C, L 337/11 of December 18, 2009.

Art.5/3 of the (e-privacy): « Confidentiality of the communications- [...]».

3. 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. »

³³ **Étienne WERY**, « Le règlement e-privacy verra-t-il le jour ? L'UE veut débloquent le dossier », article published [online] on September 26, 2019, on the website : <https://www.droit-technologie.org>, (consulted on May 13, 2025.)

See also: **The Proposals for a Regulation of the European Parliament and of the Council** on the respect for privacy and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on privacy and electronic communications), dated 10/01/2017 and 18/09/2018 and 03/10/2019. Available at the websites: <https://www.coe.int/> and <https://www.droit-technologie.org> (consulted on August 26, 2025.)

³⁴ **Étienne WERY**, « Le règlement e-privacy a (vraiment) du plomb dans l'aile ... », article published [online] on November 28, 2019, on the website : <https://www.droit-technologie.org> (consulted on June 01, 2025.)

³⁵ **Sarah SADIK**, « La protection des données dans les contrats de cloud computing », thèse de doctorat, spécialité : Droit privé, Université de Perpignan via Domitia, 23/01/2023, pp. 75-77, publié [en ligne] le 02/06/2023 sur le site: <https://theses.hal.science/tel-04114471v1> (consulté le 14/07/2025.)

³⁶ **Art.51 (GDPR)** : « **Supervisory authority**

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to

the consistency mechanism referred to in Article 63. 4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them. »

See also: the Arts. 52-58 of (GDPR).

³⁷ See also: the Arts. 52- 58 of (GDPR).

Philippe MOURON, « Nouvelles sanctions infligées à facebook en Allemagne et en Italie », article available on the website: https://www.la-rem.eu/202002/nouvelle-sanctions-infligees-a... (consulted on August 23, 2025.)

Yvonne GANGLOFF, « RGPD : l'UE a distribué 114 millions d'euros d'amendes depuis 2018 », article published [online] on January 21, 2020 at 08:08, from the following address : <https://www.seicledigital.fr/2020/01/21/rgpd-114-millions-euros-amendes/> (consulted on June 12, 2025.)

³⁸ **Cnil. Délibération** n° SAN-2019-001 du 21-01-2019, prononçant une sanction pécuniaire à l'encontre de la société Google LLC. Available on sites : <https://www.cnil.fr/>, and <https://www.legifrance.gouv.fr/affichCnil/> (accessed on May 23, 2025.)

³⁹ **Judgment of the CJEU** of October 01, 2019, (Case C- 673/17), Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV v Planet 49 GmbH. Available at: <https://www.curia.europa.eu/juris/document> (accessed on August 23, 2025.)

⁴⁰ **EC. 10th -9th combined chambers**, No. 434684, of June 19, 2020, Association of communication and other consulting agencies. Available at the website: <https://www.legifrance.gouv.fr> (consulted on July 25, 2025.)

Voir aussi : **Emmanuel WALLE**, « Cookie et autres traceurs : annulation partielle des lignes directrices de la Cnil », article published [online] on August 07, 2020, from the following address : <https://www.alain-bensoussan.com> (accessed on June 19, 2025.)

⁴¹ **Cnil**, « Cookies et autres traceurs : la Cnil publie de nouvelles lignes directrices » on 18 July 2019. Available on the website: <https://www.cnil.fr> (accessed on June 28, 2025.)

See also on this topic : **Anne MESSAS**, « « Cookiegate » : après la décision du Conseil d'État, où en sommes-nous ? », article published [online] on July 03, 2020, on the website: <https://www.taoma-partners.fr/blog/2020/07/03/cookiegate-apres-la-decision-du-conseil-detat-ou-en-sommes-nous/> ou <https://www.hmv.fr> (consulted on August 10, 2025.)

⁴² **Judgment of the CJEU** (Grand Chamber) of July 16, 2020, Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems. Available at: https://www.curia.europa.eu/jcmc/jcmc/Jo2_7052/fr/ et <https://www.eur-lex.europa.eu/legal-content/FR/> (consulted on August 14, 2025.)

⁴³ **Commission Implementing Decision (EU) 2016/1250** of July 12, 2016 in accordance with Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection afforded by the EU-US Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance) (2016/1250/EU), O.J.E.C, L 207/1, August 01, 2016. <https://www.eur-lex.europa.eu/legal-content/> (consulted on July 12, 2025.)

⁴⁴ **Commission Decision 2010/87** of February 05, 2010 on standard contractual clauses for the transfer of personal data to subcontractors established in third countries pursuant to Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593 [Text with EEA relevance] (2010/87/EU), O.J.E.C, L 39/5, February 12, 2010. <https://www.eur-lex.europa.eu/legal-content/> (consulted on June 10, 2025.)

⁴⁵ For more information on this topic, see: **Damien LELOUP, Grégor BRANDY**, « L'accord sur le transfert de données personnelles entre l'UE et les États-Unis annulé par la justice européenne », article published on July 16, 2020 at 10:32- Updated on July 16, 2020 at 19:35 on the website : <https://www.lemonde.fr/pixels/article/2020/07/16/> (consulted on July 20, 2025.)

Thomas CHENEL, « Google et Facebook ne pourront plus transférer comme avant les données des utilisateurs européens », article published [online] on July 16, 2020, at 13:02 from the following address : <https://www.businessinder.fr/> (consulted on August 23, 2024.)

⁴⁶ **Judgment of the CJEU** (Grand Chamber) of October 06, 2015, Case C-362/14 Maximilian Schrems v Data Protection Commissioner (in the presence of: Digital Rights Ireland Ltd). Available at: <https://www.curia.europa.eu/jcmc/jcmc/> and <https://www.eur-lex.europa.eu/legal-content/FR/> (consulted on June 14, 2025.)

⁴⁷ **Decision 2000/520/EC of July 26, 2000** in accordance with Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection afforded by the principles of the safe harbor and frequently asked questions relating thereto, published by the Ministry of the United States of America (notified under document number C (2000) 2441) (text with EEA relevance), O.J.E.C, L 215, August 25, 2000 (No longer in force). <https://www.eur-lex.europa.eu/legal-content/> (consulted on August 12, 2025.)

⁴⁸ For more information on this topic, see : **Nicolas OCHOA**, « La spécificité de la protection des données personnelles en matière fiscale », revue Gestion & Finances Publiques, n° 6/Novembre-Décembre 2017, pp.79, 80.

Damien LELOUP, Cécile DUCOURTIEUX, Martin UNTERSINGER, « La justice Européenne a invalidé l'accord qui encadrerait le transfert de données personnelles de l'Europe vers les États-Unis », article published [online] on October 06, 2015 at 17:53- Updated on October 07, 2015 at 10:27, on the website: <https://www.lemonde.fr/pixels/article/2015/10/06/> (consulted on April 20, 2025.)

Jérôme DEROULEZ, « De la sphère de Sécurité (« Safe Harbor ») au Bouclier de protection (« Privacy Shield ») : État des lieux à mi-parcours », article published [online] on February 2016, on the siteweb : <https://www.village-justice.com/article/sphere-securite-Safe-Harbour,21514.html> (consulted on July 23, 2025.)

⁴⁹ **Leïla SAYSSA**, « Data Privacy Framework (DPF) : troisième tentative, troisième échec ? » article published [online] on April 25, 2025 on the website : <https://www.dastra.eu/fr/article/data-privacy-framework-troisieme-tentative-troisieme-echec/59103> (accessed on August 01, 2025.)

⁵⁰ For more information on the subject, see this website: <https://www.dataprivacyframework.gov/Program-Overview> (accessed on August 20, 2025.)

Bibliography:

A - Theses :

- 1- **Imane FOUAD**. "Detection and measurement of web tracking." Doctoral thesis in Informatics, Center Inria d'Université Côte d'Azur, June 29, 2021. pp. 12-15. Published [online] on December 07, 2021 on the website : HAL Id: tel-03278529 et <https://theses.hal.science/tel-03278529v2> Submitted on 7 Dec 2021(consulted on August 02, 2025.)
- 2- **Michaël TOTH**, « Consent on the web : a transdisciplinary analysis », Doctoral thesis in Informatics, Center Inria d'Université Côte d'Azur, 19/06/2023. Published [online] on October 26, 2023, on the website : <https://theses.hal.science/tel-04259483v1>(consulted on June 02, 2025.)
- 3- **Sarah SADIK**, « La protection des données dans les contrats de cloud computing », these de doctorat, spécialité: Droit privé, Université de Perpignan via Domitia, 23/01/2023. Publiée en line le 02/06/2023 sur le site: <https://theses.hal.science/tel-04114471v1> (consulté le 14/07/2025.)

B - Newspaper articles:

- 1- **Alexandre CHEN**, « Gérer les données personnelles fournies aux applications », revue I2D - Information, données & document, volume 43, n° 3/ 2017, pp. 47 à 48.
- 2- **Alexandre SERRES**, « Problématiques de la trace à l'heure du numérique », revue Sens-Dessous, 2012/1. N° 10, pp. 84-94.
- 3- **Catherine BARREAU**, « Le marché unique numérique et la régulation des données personnelles », revue Réalités industrielles, 2016/3 Août 2016, pp. 37,41.
- 4- **Éric ANDRIEU**, « Internet et la protection des données personnelles », revue LEGICOM, Jun 2000/1 n° 21-22, pp. 155-166. DOI: 10.3917/legi.021.0155
- 5- **Nicolas OCHOA**, « La spécificité de la protection des données personnelles en matière fiscale », revue Gestion & Finances Publiques, n° 6/Novembre-Décembre 2017, pp.75, 80.
- 6- **Valérie LAURE BENABOU**, « L'extension du domaine de la donnée », revue LIGECOM 2017/2 N° 59, pp. 03-17. DOI: 10.3917/legi.059.0003

C - Legal Texts:

- 1- **Regulation (EU) 2016/679** of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)), Official Journal of the European Union L 119/1 of May 04, 2016.
- 2- **Directive 2002/58/EC** of the European Parliament and of the Council of July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O.J.O.C.E, L 201/37 of July 31, 2002.
- 3- **Directive 2009/136/EC** of the European parliament and of the Council of November 25, 2009, amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, O.J.E.C, L 337/11 of December 18, 2009.
- 4- **Decision 2000/520/EC** of July 26, 2000 in accordance with Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection afforded by the principles of the safe harbor and frequently asked questions relating thereto, published by the Ministry of the United States of America (notified under document number C (2000) 2441) (text with EEA relevance), O.J.E.C, L 215, August 25, 2000 (No longer in force). <https://www.eur-lex.europa.eu/legal-content/>
- 5- **Commission Decision 2010/87** of February 05, 2010 on standard contractual clauses for the transfer of personal data to subcontractors established in third countries pursuant to Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593 [Text with EEA relevance] (2010/87/EU), O.J.E.C, L 39/5, 12.02.2010. <https://www.eur-lex.europa.eu/legal-content/>
- 6- **Commission Implementing Decision (EU) 2016/1250** of July 12, 2016 in accordance with Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection afforded by the EU-US Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance) (2016/1250/EU), O.J.E.C, L 207/1, 01.08.2016. <https://www.eur-lex.europa.eu/legal-content/>

D- Websites:

- 1- **Arnaud JACQUES**, « Les Cookies informatiques et la sécurité », pp. 05-08, article published [online] on July 15, 2002, on the website: <https://www.securiteinfo.com/conseil/cookies/shtml> (consulted on June 04, 2025.)
- 2- **Anne MESSAS**, « « Cookiegate » : après la décision du Conseil d'État, où en sommes-nous ? », article published [online] on July 03, 2020, on the website: <https://www.taoma-partners.fr/blog/2020/07/03/cookiegate-apres-la-decision-du-conseil-detat-ou-en-sommes-nous/> ou <https://www.hmv.fr> (consulted on August 10, 2025.)
- 3- **B. BATHELOT**, « Cookies tiers », article published [online] on March 18, 2020, on the website: <https://www.definition-marketing.com/definition/cookie-tiers/> (accessed on August 02, 2025.)
- 4- **CNIL**, « Cookies et autres traceurs : la Cnil publie de nouvelles lignes directrices » le 18 juillet 2019. Available on the website: <https://www.cnil.fr> (consulted on June 28, 2025.)
- 5- **CNIL**: « Les durées de conservation des données », published July 28, 2020, on the website: <https://www.cnil.fr/fr/passer-laction/les-durees-de-conservation-des-donnees/> (consulted on August 04, 2025.)
- 6- **CNIL**: « Cookies & traceurs: que dit la loi ? », published on [online] on the website: <https://www.cnil.fr/fr/cookies-traceurs-que-dit-la-loi> (accessed on June 14, 2025.)
- 7- **CNIL**. Délibération n° SAN-2019-001 du 21-01-2019, prononçant une sanction pécuniaire à l'encontre de la société Google LLC. Available on sites : <https://www.cnil.fr/>, and <https://www.legifrance.gouv.fr/affichCnil/> (accessed on May 23, 2025.)
- 8- **Cookiebot** : « Cookies Internet : Que sont-ils et que font-ils ? », cookiebot.com, article published [online] on February 24, 2020, on the website : <https://www.cookiebot.com/fr/cookie-internet/> (consulted on January 12, 2025.)
- 9- **Damien LELOUP, Cécile DUCOURTIEUX, Martin UNTERSINGER**, « La justice Européenne a invalidé l'accord qui encadrait le transfert de données personnelles de l'Europe vers les Etats-Unis », article published [online] on October 06, 2015 at 17:53- Updated on October 07, 2015 at 10:27 on the website: <https://www.lemonde.fr/pixels/article/2015/10/06/> (consulted on April 20, 2025.)
- 10- **Damien LELOUP, Grégor BRANDY**, « L'accord sur le transfert de données personnelles entre l'UE et les États-Unis annulé par la justice européenne », article published [online] on July 16, 2020 at 10:32- Updated on July 16, 2020 at 19:35 on the website : <https://www.lemonde.fr/pixels/article/2020/07/16/> (consulted on July 20, 2025.)
- 11- **Emmanuel WALLE**, « Cookie et autres traceurs : annulation partielle des lignes directrices de la Cnil », article published [online] on August 07, 2020, from the following address: <https://www.alain-bensoussan.com> (accessed on June 19, 2025.)
- 12- **Étienne WERY**, « Le règlement e-privacy a (vraiment) du plomb dans l'aile ... », article published [online] on November 28, 2019 on the website : <https://www.droit-technologie.org> (consulted on June 01, 2025.)
- 13- **Étienne WERY**, « Le règlement e-privacy verra-t-il le jour ? L'UE veut débloquent le dossier », article published [online] on September 26, 2019, on the website: <https://www.droit-technologie.org> (consulted on May 13, 2025.)
- 14- **Etienne WERY, Olivia GUERGUINOV**, « Combien de temps peut-on conserver des données personnelles ? », article published [online] on September 01, 2020, from the following address: <https://www.droit-technologie.org/actualites/> (consulted on July 12, 2024.)
- 15- **FDPIC report** (Federal Data Protection and Information Commissioner) on the "New developments in cookies", p. 02, published [online] at:

- <https://www.edoeb.admin.ch/content/edoeb/fr/home/documentation/rapports-d-activites/anciensrapports/18eme-rapport-d-activites-2010-2011/nouvelle-evolution-des-cookies.pdf> (accessed on June 25, 2025.)
- 16- **FDPIC' document** on : « Explications concernant le webtracking ». August 2013, pp. 01-05. Available on: https://www.edoeb.admin.ch/content/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/explication-le-webtracking-.pdf (consulted on January 25, 2025.)
 - 17- **Gabriel Dabi- SCHWEBEL**, « Tracker et tracking : définition (appliquées au web), article published [online] on November 14, 2024 on the website: <https://www.1min30.com/dictionnaire-du-web/tracker-et-tracking/> (accessed on March 20, 2025.)
 - 18- **Gary DAGORN**, « Cookies, mouchards : comment vous êtes suivis sur internet », article published [online] on March 30, 2018 at 15:24- Updated on October 14, 2019 at 11:33, from the following address : <https://www.lemonde.fr/les-decodeurs/article/2018/03/30/> (consulted on June 20, 2025.)
 - 19- **Grégory JEANDOT**, « Les cookies pour les nul en informatique », article published [online] on March 14, 2013 - Updated on March 20, 2013 at 17:13, from the following address : <https://www.e-marketing.fr/Theematique/data-1091/Tribune/Les-cookies-nule-informatique-229748.htm> (accessed on June 12, 2025.)
 - 20- **Google Operator document** on: "Delete, allow and manage cookies in Chrome", published on 2025, from the following address: https://support.google.com/chrome/answer/95647?hl=en-gb&p=cpn_cookies (accessed on August 12, 2025.)
 - 21- **Jean-LUC MARINI**, « Le tracking est-il dangereux ? », article published [online] on March 08, 2016 at 11:00, from the following address : <https://www.journaldunet.com/ebusiness/crm-marketing/117524/> (consulted on August 21, 2025.)
 - 22- **Jérôme DEROULEZ**, « De la sphère de Sécurité (« Safe Harbor ») au Bouclier de protection (« Privacy Shield ») : État des lieux à mi-parcours », article published [online] in February 2016, on the website: <https://www.village-justice.com/article/sphere-securite-Safe-Harbour,21514.html>(consulted on July 23, 2025.)
 - 23- **CNIL** : « Cookies et traceurs : comment mettre mon site web en conformité ? », published [online] on October 01, 2020, on the: <https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/comment-mettre-mon-site-web-en-conformite> (accessed on June 14, 2025.)
 - 24- **Leïla SAYSSA**, « Data Privacy Framework (DPF) : troisième tentative, troisième échec ? » article published [online] on April 25, 2025 on the website : <https://www.dastr.eu/fr/article/data-privacy-framework-troisieme-tentative-troisieme-echec/59103> (accessed on August 01, 2025.)
 - 25- **Ludwig HERVÉ**, « Décryptage : les techniques de tracking avancées et les enjeux de la protection des données », article published [online] on May 16, 2017 at 09:59, updated on December 29, 2017, from the following address: <https://www.blogdumoderateur.com/tracking-enjeux-protection-donnees/> (consulted on July 09, 2025.)
 - 26- **Peter TRUDEAU**, « Qu'est-ce que le Web Tracking ? Et les trackers dans les navigateurs ? », article published [online] on May 24, 2020, on the website: <https://windowsastuce.com/> (accessed on July 12, 2025.)
 - 27- **Philippe MOURON**, « Nouvelles sanctions infligées à facebook en Allemagne et en Italie », article available on the website: <https://www.la-rem.eu/202002/nouvelle-sanctions-infligees-a.../> (consulted on August 23, 2025.)

- 28- **Sylvain MÉTILLE**, « les cookies en droit suisse », published [online] on February 08, 2025, on the website : <https://smetille.ch/2025/02/28/cookies-droit-suisse/> (consulted on June 10, 2025.)
- 29- **Thierry Léonard, Olivia GUERGUINOV, Etienne WERY**, « C'est quoi le consentement en matière de cookies et données personnelles ? », article published [online] on June 10, 2020, on the website: <https://www.droit-technologie.org> (accessed on July 02, 2025.)
- 30- **Thomas CHENEL**, « Google et Facebook ne pourront plus transférer comme avant les données des utilisateurs européens », article published [online] on July 16, 2020 at 13:02 from the following address: <https://www.businessinder.fr/> (consulted on August 23, 2024.)
- 31- **Yvonne GANGLOFF**, « RGPD : l'UE a distribué 114 millions d'euros d'amendes depuis 2018 », article published [online] on January 21, 2020 at 08:08, from the following address: <https://www.seicledigital.fr/2020/01/21/rgpd-114-millions-euros-amendes/> (consulted on June 12, 2025.)
- 32- **Arrah-MARIE JO**, « Les effets inattendus du RGPD sur la concurrence dans le marché de la publicité en ligne », *hal.science*, pp. 01-12, article published [online] on October 06, 2024, on the website: <https://hal.science/hal-04315721v1> (accessed on August 10, 2025.)

E- Jurisprudence :

- 1- Judgment of the CJEU (Grand Chamber) of October 06, 2015, Case C-362/14 Maximilian Schrems v Data Protection Commissioner (in the presence of: Digital Rights Ireland Ltd). Available at: <https://www.curia.europa.eu/jcmc/jcmc/> and <https://www.eur-lex.europa.eu/legal-content/FR/> (consulted on June 14, 2025.)
- 2- Judgment of the CJEU of October 01, 2019, (Case C- 673/17), Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV v Planet 49 GmbH. Available at: <https://www.curia.europa.eu/juris/document> (accessed on August 23, 2025.)
- 3- Judgment of the CJEU (Grand Chamber) of July 16, 2020, Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems. Available at: https://www.curia.europa.eu/jcmc/jcmc/Jo2_7052/fr/ et <https://www.eur-lex.europa.eu/legal-content/FR/> (consulted on August 14, 2025.)
- 4- EC. 10th -9th combined chambers, No. 434684, of June 19, 2020, Association of communication and other consulting agencies. Available at: <https://www.legifrance.gouv.fr> (consulted on July 25, 2025.)