GDPR, ACT II

COLLECTIVE CONTROL OF OUR DATA AS AN IMPERATIVE

Jean Rérolle, Julia Roussoulières

THINK-TANK DIGITAL NEW DEAL

May 2022

SIMILARLY TO ENVIRONMENTAL PROTECTION, PERSONAL DATA PROTECTION IS A COLLECTIVE PROBLEM AND MUST BE TREATED AS SUCH "

SUMMARY

PREFACE

Rarely has a European regulation been as visible and known to European citizens as the GDPR. The debate surrounding it is very lively: it is often taken as an example of the success of European *soft power*. European law would finally play the game of American extra-territoriality, by promoting a real framework for data sharing.

However, the latest condemnations by the CNIL show that even the biggest players, such as Google, are not in compliance with either the GDPR or with previous regulations, such as ePrivacy. It is also easy to see that "classic" companies are most often lacking the tools to apply it and that users, already tired of the banners asking for consent, are little aware of what is really happening to their data.

With data sharing at an all-time high and lacking transparency in the online advertising market, it is time to take another look at the GDPR.

Over the course of several months of investigation, the authors followed the trail of their personal data to find that many of the rights conferred by the GDPR were not effective and that individual consent was an insufficient approach. Does this mean we should throw everything away?

Certainly not! We can start with simple measures to improve the implementation of the GDPR. Above all, by putting collectivity at the service of personal data, with more collective actions and greater involvement of civil society. But also by making courageous political choices, especially concerning regulation of online advertising.

We are convinced that it is now time to consider a real Act II of the Regulation with the arrival of the European package DSA, DMA, DGA, and DataAct. The GDPR will be able to reach its full power by relying on the Data Strategy and, at last, become a true general regulation for all data.

Axelle Lemaire,
Former Secretary of State for the Digital Economy and Innovation
Director of Strategy, Transformation and Innovation at the Red Cross
Member of the board of the Digital New Deal think-tank.

SUMMARY

As digital tools develop, the extent to which personal data is collected and processed continues to grow. For some, this has fuelled fears of privacy intrusion by the state or private actors, but also of discrimination, surveillance or manipulation.

The European regulatory response, the General Data Protection Regulation (GDPR), which aims to ensure both the protection of data and its free flow, has been welcomed worldwide. However, the collection and sharing of personal data continues to grow, driven by the needs of online advertising, and still remains on a scale that is not well understood by citizens. While the GDPR has undoubtedly helped to bring the subject a little more into the daily lives of European internet users, for many it is synonymous with a degraded experience, red tape and a regulatory black box.

Four years after the GDPR came into force, we are of the view that it has not reached its full potential to protect citizens and meet their expectations: there is still a lot to do!

We propose ways to remedy the shortcomings of the GDPR: by improving the user experience and by reinforcing the free and informed nature of consent. Beyond the individual rights it confers, we propose to complete it with the possibility of collective action, by involving civil society more, and by better articulating individual consent and collective choices.

“THE MASS OF VERY PRECISE DATA COLLECTED TODAY BY PRIVATE COMPANIES, AS WELL AS THEIR PREDICTIVE POWER, OPENS UP THE POSSIBILITY OF THEIR USE BY STATES OR MALICIOUS GROUPS”

I. PROBLEMATIC DATA COLLECTION

In 2020, 90% of French people used the internet[1]. 80% of them did so daily. Of these internet users, 72% used a social network and 70% made online purchases. In doing so, they have shared a large amount of personal data with private actors.

WHAT IS PERSONAL DATA?

The CNIL, *Commission Nationale de l'Informatique et des Libertés*, defines personal data as follows: "*Personal data is any information relating to an identified or identifiable natural person*".

Personal data is diverse. Some personal data is voluntarily and consciously shared by the user with a site through forms and subscriptions: name, first name, date of birth, etc. Other data is shared in a way that is less easily perceptible to the internet user: this is data that is observed, in particular through cookies and which constitutes digital traces.

From this data, information about individuals can be inferred: age, income level, family structure, political preferences, etc. This information can then be reworked, shared and exploited to drive recommendation or prediction algorithms.

WHAT IS A COOKIE?

A cookie is a small computer file stored on a device during online browsing, which allows identification and tracking of an internet user. Cookies can contain a lot of observed data, such as information about your browser, your location, or the last time you visited a particular site.

THE EXTENT OF DATA COLLECTION, PROCESSING AND SHARING IS NOT WELL-KNOWN

Although the systematic consent banners (where the user is asked to accept or refuse cookies) have made the monitoring of online browsing visible, the scope of the collection and the number of actors involved are generally unknown to internet users. Indeed, this collection can range from simple cookies to the precise and continuous location of the user, while the number of actors collecting data on a simple press site can be as high as several hundred[2].

In the field of mobile applications, a study by the Norwegian consumer association Forbruker Radet[3] has highlighted the massive data collection and sharing carried out by applications on users' smartphones.

The association analysed the data flows emitted by 10 applications and their recipients. It found that the LGBT+ dating app Grindr collects and then shares its users' identities as well as location data or specific sexual preferences with around 20 advertising partners, without the user being clearly informed or being able to object. The same applies to the Muslim Assistant application, which shares the location and identity of its users with numerous partners. In both cases, being a user of the application is sensitive personal data as it reveals information about religion or sexual orientation. Grindr was fined €10 million

[1] *Référentiel des usages numériques, Février 2021, CSA-ARCEP, online.*
[2] *For example 700 on www.lefigaro.fr, or even 426 on www.lequipe.fr.*
[3] *Out of controll, Forbruker Radet, 01/2020, online.*

by the Norwegian Data Protection Authority as a result of this investigation[4].

The personal data collected in this way by applications or websites is shared with other companies: advertising partners, technology companies, but also companies from the "physical" world, far from GAFAM[6] alone, often the only ones criticised for their data management. This data also frequently passes through the hands of intermediaries less well-known to the general public: the data brokers.

These data brokers base their business models on the resale and sharing of data collected from various sources. One of them, LiveRamp, is the partner of press sites such as Le Monde, Le Figaro, L'Équipe or even retail players like Carrefour. The reading of an article or the act of purchase by an individual is information that LiveRamp can then share with its partners without the individual concerned being informed.

THE DRIVER OF COLLECTION: ONLINE TARGETING

The online advertising market is the main consumer of personal data. This is due in particular to the programmatic advertising mechanism used to assign an ad to an internet user. This market finances most digital services, which are therefore free to the user.

At the beginning of the 20th century, the advertiser Jon Wanamaker said: "I know that half of my advertising investment is wasted; the problem is that I don't know which half". The promise of individualised targeted advertising is to get rid of that unproductive half of advertising spend by targeting only customers whose potential interest in the product is known in advance.

THE PROGRAMMATIC CHAIN OF ONLINE ADVERTISING

When the user connects to a page on a publisher's site, an auction is organised for the right to display an advertisement in the different possible spaces on the web page. Each potential advertiser places a bid, based on the value they place on the user. The advertiser estimates this value based on the information it has about the user. The more data they have, the more accurate they can be in estimating the bid to be placed, which is why they may sometimes purchase additional data from a data broker, such as LiveRamp. There are many companies that specialise in different stages of the advertising process, forming an ecosystem called AdTech.

[4] *20 minutes, En Norvège, Grindr pourrait payer cher, 2020, online.*

Figure 1: The players in online advertising.

Source : Autorité de la Concurrence.

Personal data is also used to drive different algorithms. In particular, they make it possible to propose individualised product recommendations, or to estimate the price that a customer is prepared to pay for a product, and therefore whether or not it is relevant to offer him a price reduction: this is a form of price discrimination.

For the user, the output of these algorithms, i.e. the advertisements he sees, the products that are recommended to him and the prices that are offered to him, are the only manifestation of the generalised use of his data that is made by the various digital actors.

WHY IS THIS A PROBLEM?

These manifestations of data use do not inform the user about the extent of data collection and sharing. This lack of understanding about the scope and wide variety of actors sharing data fuels a great deal of fear.

Firstly, some people fear for their privacy, for example not wanting confidential or compromising information about them to be disclosed. In the case of the study conducted by the Norwegian consumer association, Forbruker Radet[5], this fear is reinforced by the sensitivity of the information held by the applications studied (sexual orientation, religion).

Secondly, there are fears about the possibilities of **discrimination** offered by the knowledge of personal data. The opacity of certain algorithms does not make it easy to bring these phenomena to light and numerous research studies have already shown cases of **voluntary** discrimination – Facebook, in particular, was sued by the US Department of Housing for having allowed advertisers to limit the visibility of housing offers to people of a certain origin[6] - and of **involuntary** discrimination caused by biases in the very structure of the algorithms[7].

Fear of a new form of **surveillance** subsequently emerged. Edward Snowden's revelations in 2013 revealed the means used by the American state to monitor its citizens[8]. The mass of very precise data collected today by private companies, as well as their predictive power, opens up the possibility of their use by states or malicious groups - for example, the American state has bought geolocation databases from private companies to monitor its borders[9].

Finally, this wealth of individual information can be used for **manipulation** purposes. The predictive power granted by the very detailed knowledge of internet users[10] gives the largest

[5] *Out of controll, Forbruker Radet, 01/2020, online*
[6] *Facebook sued for discrimination by US housing department, Les Echos, 2019, online.*
[7] *"Algorithms: preventing the automation of discrimination", Human Rights Defender, 2020, online. https://www.lemonde.fr/pixels/article/2019/09/13/ce-que-les-revelations-snowden-ont-change-depuis -2013_5509864_4408996.html*
[8] *https://www.lemonde.fr/pixels/article/2019/09/13/ce-que-les-revelations-snowden-ont-change-depuis-2013_5509864_4408996.html*
[9] *Federal agencies use cell phone Location Data for Immigration Enforcement, The Wall Street Journal, 2020, online.*
[10] *See the book by lawyer and Harvard law professor: Zuboff, S., The Age of Surveillance Capitalism, 2020.*

digital companies an “instrumentation power” that enables them to influence the behaviour of individuals. While this influence is currently mainly manifested in purchasing behaviour, the Cambridge Analytica scandal and the theories associated with it highlight a variety of political and social uses that could materialise from holding knowledge about individuals. Online advertising and recommendation algorithms, through their extreme personalisation, already make it possible to convey messages adapted to an audience and to “information bubbles”[11].

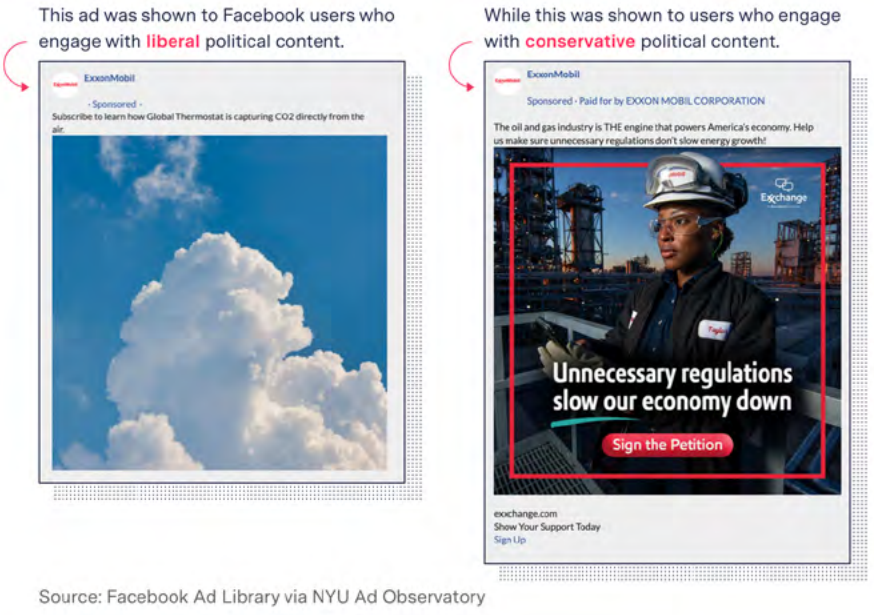


Figure 2 : ExxonMobil shows very different advertisements to targets with opposing political sensitivities.
Source : The Markup.

[11] *How Facebook's ad system lets company talk out both sides of their mouths, The Markup, 2021, online.*

THE RGPD WILL REACH ITS FULL POTENTIAL IF WE CORRECT ITS SHORTCOMINGS AND ESPECIALLY IF WE GO FURTHER WITH A COLLECTIVE APPROACH TO DATA"

II. THE PUBLIC RESPONSE: BETWEEN COMPETITION POLICY AND TREATMENT REGULATION

Public action mobilises two main levers to enable the protection of personal data: the framework of personal data processing and competition policy tools. The news focuses on the new competition policy tools, but has the GDPR said its last word?

REGULATION OF PLATFORMS

Digital platforms, the most iconic of which are GAFAM, concentrate and collect large quantities of personal data. Through their dominant positions, they lock up the market and can set their terms of service in terms of respect for the personal data of captive citizens.

Faced with the limits of traditional competition policy, the European Union has decided to adopt new legislation allowing for asymmetrical regulation of so-called "structuring" platforms in order to limit their market power. This European legislation is notably comprised of the Digital Markets Act (DMA) and the Digital Services Act (DSA) and constitutes a real paradigm shift for European competition policy, which should be evaluated in the coming years.

Increased competition can have positive effects for the protection of personal data by allowing the citizen to choose a service with suitable privacy conditions. Conversely, data protection and competition regulation may conflict: accumulated user data gives the company in possession of it a competitive advantage, and the competition authority may want to compel the company to allow access to it for competition. Therefore, decisions strengthening data protection may have strong anti-competitive consequences[12].

However, the interactions between competition and data protection are too complex for competition policy to be the only weapon used for this purpose[13].

SUPERVISION OF PERSONAL DATA PROCESSING

The CNIL was created in France in 1976 following fears surrounding the surveillance of the French people as a result of the Safari project[14]. Since then, it has been an independent administrative authority responsible for enforcing laws on the protection of personal data. Article 8 of the European Charter of Fundamental Rights guarantees every European citizen the right to protection of his or her personal data. These rights and the rules to be followed regarding the protection of personal data in the European Union are mainly defined in the General Data Protection Regulation, the GDPR. The GDPR, which was voted on in 2016 and came into force in 2018, has three objectives.

The first is to ensure the free flow of data within the European Economic Area.

The second is to regulate the practices of data processors, particularly companies operating in Europe, by specifying the legal basis on which an entity may process data and the precautions it must take according to the risk that the data processing constitutes. The collection of user

[12] *Google Chrome's Privacy Sandbox project, which is supposed to improve privacy protection on the browser, has potentially important consequences for online advertising players. See Gérardin D., Google as a de facto Privacy Regulator: Analyzing Chrome's Removal of Third-party Cookies from an Antitrust Perspective, TILEC Discussion Paper, 2020, online.*

[13] *Tucker, C., Marthews A., Privacy policy and competition, Economic Studies at Brookings, 2019, online.*

[14] *The Safari project, which created a large administrative file referencing all French people via their INSEE number, aroused great opposition at the time, notably in a famous article: Safari ou la chasse aux Français, Le Monde, 1974.*

consent, which is one of the six legal bases for processing, must be explicit, free and informed and is more strictly framed, giving rise to the "accept cookies" button banners on websites. For offenders, the Regulation provides for fines of up to 50 million euros or 4% of global turnover, much higher than was previously possible.

Finally, it guarantees citizens inalienable rights over their data, such as the right to be informed about who processes their data, the right to access, rectify, oppose in certain cases, the right to portability, etc[15].

This Regulation has had a worldwide influence and has been adapted in more or less similar forms in various countries or regions, from California to Brazil. For this reason, it often represents a success for European influence on the international scene.

The GDPR has contributed to the awareness of internet users on the subject of personal data: in 2019, and after the great media campaign that accompanied its entry into force, 70% of users declared being more sensitive than before[16]. In reality, and from the point of view of the citizen's daily experience, the influence of the GDPR has mainly manifested itself via the consent collection banners that have become compulsory on all websites wishing to use cookies.

So, as the Digital Markets Act is about to come into force, it is time to take another look at the GDPR. **It has not yet reached its full potential as a result of two major flaws.**

Firstly, not all the rights conferred by the GDPR are now effective. Indeed, despite the right to information, no internet user can claim to know all the actors in possession of their data. Without knowing all of the actors, he or she cannot know all of the data that is exchanged about him or her either. Exercising the right of access is often tedious and requires patience and courage. The user experience of exercising one's rights is out of proportion to the usual standards of digital services.

On the other hand, the notion of consent is misused, rarely complying with the requirements of the GDPR because it is neither free nor informed, and moreover its experience is unpleasant for the user. Additionally, consent alone is not sufficient to address all data sharing situations. The use of legitimate interest is also unclear and open to abuse, and should be clarified.

Firstly, **we propose correcting these shortcomings by improving the implementation** of the GDPR and, secondly, we propose going even further with a **collective approach to data.** This is how the GDPR will reach its full potential.

[15] Regulation (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, online.
[16] IFOP survey conducted in April 2019 on a representative sample of 1,000 people, online.

IT IS NECESSARY TO PUT AN END TO THE STATUS OF "CO-PROCESSORS OF PERSONAL DATA" FOR ONLINE ADVERTISING PRACTICES"

III. CORRECTING THE SHORTCOMINGS OF THE GDPR

IMPROVING THE EFFECTIVENESS OF RIGHTS

We will illustrate the difficulties of exercising rights with an example. We wanted to check for ourselves whether one of the data brokers, LiveRamp, held information about us: we therefore exercised our right of access, conferred by the GDPR, with this company. In practice, this meant sending an email with our request and proof of identity and waiting 3 weeks for a response. The exercise is described in Annex 1.

LiveRamp, a company that the average user is not aware of because it does not provide a service directly to them, possesses a lot of data on us (name, address, phone number) and has inferred a certain amount of information (age, income level, family situation), which is sometimes incorrect. The source of this data is not indicated. Only the source of the postal address is indicated, a company called IG Conseil, also unknown to the user. No contact details for this company are available online, so it is necessary to ask LiveRamp for contact information.

When contacted, IG Conseil indicated that it was only an intermediary between LiveRamp and a third, unnamed company, but whose e-mail address revealed that it was Cap Décision, an SME in the Val d'Oise. When asked about the origin of the data, this company simply replied that it had been deleted, which was not the purpose of our request. The screenshot provided seems to indicate that the source of the data is a company called Edentify, which owns the Focus-news.fr website. When contacted, this company did not respond. A complaint to the CNIL has been filed.

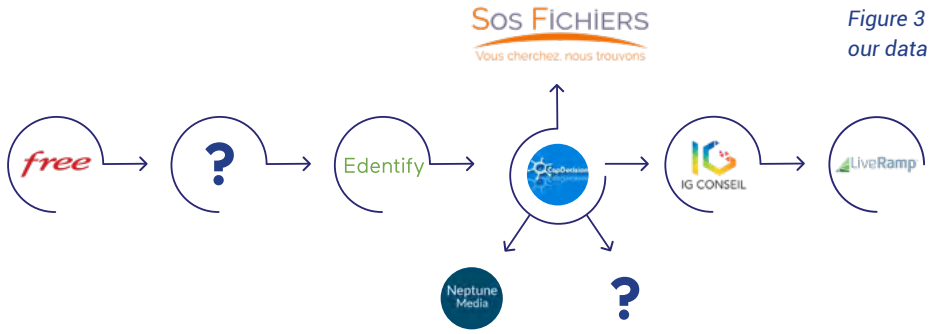


Figure 3 : The path traveled by our data

There are many elements that impede the user experience when exercising their rights. These are essential because they have the potential to convince the user to trust a service and they can enable civil society to shed light on the practices of companies.

In order to improve the exercise of rights, we first believe that it is necessary to put an end to the status of "co-processors of personal data" for online advertising practices. This status allows two actors to collect and process the same data without taking responsibility for each other, and may be quite relevant for certain situations, such as the exploitation of data from an autonomous vehicle, which could be co-processed by the vehicle manufacturer and the driver's insurer for example.

In the context of online advertising, however, this legal framework seems to be completely misused: the providers of services to the user (typically, the press publisher) associate their own advertising service providers as co-processors of data (designated as "partners" in the privacy policies), and not as sub-processors. As a result, in order to exercise the right of access to his or her data, the user must contact all the co-processors: as a rule, several hundred. It is therefore impossible in practice for the user to know who is processing his or her data - potentially several hundred actors for each article read - and even more so to access it.

Removing the possibility of co-processing would allow the user to address only the company providing the service, the only one he is really in a position to know, in order to exercise his rights. By forcing the formalisation of data exchange links between the players and their respective responsibilities, we also anticipate a reduction in the number of players involved in the advertising supply chain. At present, the advertising agencies of mainstream media indicate that they only know about a hundred players out of the half a thousand listed as "partners". The lack of legal risk in adding partners as co-processors is fuelling the inflation in the number of companies collecting personal data.

It also seems necessary to strengthen the quality requirement for what is provided by companies during the right of access, in particular in order to allow the traceability of data exchanges. In current practice, companies do not indicate to whom the data has been transmitted, nor where they come from, reinforcing a feeling of opacity about the transactions, and not making it possible to ensure that no illegally obtained data is used.

The user experience of exercising rights could be improved by drawing inspiration from the Signal Conso tool set up by the DGCCRF for consumer complaints about product non-compliance. Exchanges between citizens and businesses take place under the aegis of the regulator, which allows for rapid intervention in the event of a dispute, and drastically limits the number of cases where a complaint is actually necessary for the citizen to win their case.

Finally, improved cooperation between European regulators is necessary to ensure that complaints are dealt with with the same efficiency and within reasonable time limits, regardless of the country in which the company processing the data has chosen to be domiciled. This could involve a possible subsidiarity mechanism with a European regulator for the most important personal data management companies.

IMPROVING THE USE OF CONSENT

CONSENT IS OFTEN MISUSED

The GDPR reinforces the notion of **consent**, already introduced in the Data Protection Act, by defining it as follows in Article 4: "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".

Article 6 of the GDPR recognises consent as one of the six legal bases for data processing, alongside legitimate interest, public interest and the performance of a contract.

Today, we believe that consent has been misused for several reasons.

The user experience is bad. The daily experience of pop-up banners asking the user for information is a source of annoyance. Users express a certain weariness. This "consent

fatigue" even leads some internet users to install automated tools that accept all cookies[17].

Consent is neither free nor informed. The General Conditions of Use (GCU) are long (it would take the average internet user 76 hours a year to read all the GCU[18]) and contain technical terminology that makes them difficult to read and understand.

Furthermore, interfaces are often constructed in such a way as to push the internet user to accept the GCU, in particular via deceptive or manipulative interface designs. This is known as dark patterns: these practices are not formally prohibited, but they can go against free and informed consent[19].

Figure 4 : An example of dark patterns.

The user has no choice

Freedom of consent is also a condition for the existence of a real choice[20]. Access to certain services may be conditional on the sharing of data when the user has no other alternative: this may be the case for structuring digital platforms, but also when the service is a press site and reading an article cannot be done on another site.

A further step has been taken with the appearance of cookie walls. This time, the user is offered two alternatives: either he accepts the conditions for sharing his data, or he pays for the service. This solution, which is very common on online press sites, is not illegal either. Even if the CNIL wanted to prohibit it via its guidelines[21], the Council of State ruled that the legality of this practice had to be decided on a case-by-case basis: "*the freedom of consent of individuals must be assessed on a case-by-case basis, taking into account in particular the existence of real and satisfactory alternatives offered in the event of refusal of cookies*".

Figure 5 : An example of a cookie wall.

Source : Screenshot from the Marmiton.fr website

Whether consent is in place or not, **it is sometimes not respected at all**. Indeed, some sites allow themselves to share their visitors' data even before they have consented or not, others share data despite consent[22].

[17] *For example, the browser extension 'I don't care about cookies', online.*
[18] *A. McDonald et al., « The Cost of Reading Privacy Policies », A Journal of Law and Policy, 4 /3, 2008, p. 543-568, online.*
[19] *A study of consent banners on 10,000 sites showed that only 11.8% of them were compliant with the GDPR because they met three cumulative criteria: (i) the explicit nature of the consent, for example via the presence of a button; (ii) the equal simplicity between "accept all" and "refuse all"; (iii) the absence of a pre-ticked box in favour of consent. See M. Nouwens et al, "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence", Conference on Human Factors in Computing Systems, 8 January 2020, online.*
[20] *Recital 42 of the GDPR expresses this: "Consent should not be considered to have been given freely if the data subject does not have a genuine choice or is not able to refuse or withdraw consent without suffering harm."*
[21] *The CNIL's concerns about cookie walls, in particular about monetisation and its risks, are very well summarised in an article by the regulator, online.*
[22] *This is what Pixel de Tracking shows in an article full of bad examples, online.*

WHEREAS CONSENT IS TODAY, IT IS NECESSARY TO IMPROVE IT AND TO MAKE IT MORE IN ACCORDANCE WITH ITS OBJECTIVES INITIAL.

Considering that consent is now being misused, it is necessary to improve it and make it more in line with its original objectives.

IMPROVING THE USER EXPERIENCE

Rather than systematising the acceptance or refusal of cookies, it is possible to act on the user experience. For example, the forthcoming ePrivacy Regulation plans to centralise the setting of consent preferences directly on the browser. This decision raises many competition issues and has been opposed by publishers. Publishers want to keep a direct link with their customers and fear that the browser settings will be biased by Google and Apple, which account for 90% of the market, for example by nudging users to accept tracking from Google and not from other companies. In order to avoid this situation, we recommend that the browser be included in the scope of the DMA and DSA structuring platforms, and that the regulator be able to object to an anti-competitive technical change.

Figure 6 : Elon Musk dreamed it, Europe did it.
Source : Twitter

BY MAKING IT FREER AND MORE ENLIGHTENED:

The CNIL wanted to make these designs more balanced via new guidelines that came into force in April 2021 (see Figure 6). This modest change, although still little respected, has in itself upset the rate of consent: the Syndicat des Régies Internet (SRI) estimates that it leads to a fall in consent of between 30 and 60 points.

These new guidelines and the proliferation of misleading designs require further capacity

building within the regulatory bodies in this area, as well as the provision of automated tools for detecting abusive designs.

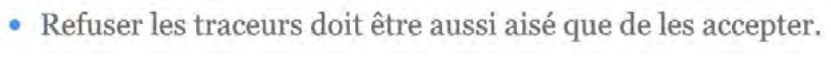


Figure 7 : The new CNIL guidelines.
Source : CNIL

The NOYB organisation is taking the lead in this area and has announced that it has issued more than 500 formal notices to sites that do not comply with CNIL guidelines, using an automated detection tool similar to this one[23].

In order to inform users' choices, we also believe it is imperative to continue to raise awareness and provide citizens with good information on the issues surrounding personal data. Ignorance of the extent of data collection and sharing is not inevitable and we believe it is essential to develop a data culture. Several avenues can be explored to improve information and strengthen training or communication campaigns, particularly via digital awareness-raising schemes in schools such as the Pix initiative.

BY GIVING THE CHOICE

In the digital space, citizens are often captive to services with strong network effects and therefore natural monopolies, which can consequently set their terms of service, including privacy policies. In order to enable citizens to choose services that suit them, various actions can be envisaged to bring about alternatives.

The right to portability, enshrined in the GDPR, is struggling to be mobilised in practice due to numerous obstacles. Common international standards are lacking to allow fluid exchanges, and initiatives such as Gaïa-X (in Europe) or the Data free-flow with Trust (led by Japan) are necessary and must be supported. In order to encourage citizens to use their right to portability, they can set up a "Blue button" which will allow them to export their data, similar to what was set up by the Obama administration for health data.

Finally, public support for the innovative ecosystem of "trusted third parties", which aim to make the user experience of changing services and reusing data more fluid, could be strengthened. Various levers could be used, such as facilitating their inclusion in public orders, strengthening and generalising their partnerships with local players and authorising data recovery by scraping methods in the framework of the Data Governance Act.

[23] *https://www.lemonde.fr/pixels/article/2021/05/31/cookies-sur-internet-des-militants-a-l-offensive-cont re-la-terreur-des-traceurs-informatiques_6082155_4408996.html*

“

POWER IS UNBALANCED BETWEEN THE INDIVIDUAL AND THE COMPANIES REQUESTING CONSENT”

IV. SUPPLEMENTING THE GDPR WITH A COLLECTIVE APPROACH

QUESTIONING INDIVIDUAL CONSENT

Consent is easily misused and despite the opportunities identified to improve it, the relevance of this concept in the field of targeted advertising should be questioned.

FIRST OF ALL, WHY RESORT TO CONSENT?

The notion of privacy is complex[24] and contextual[25]: it does not mean the same thing to everyone and can be expressed differently depending on the situation. Traditionally, the right to privacy has been defined as a "right to be left alone"[26] and without intrusion into one's private sphere. The notion has also evolved to encompass the idea of informational self-determination: each individual is free to choose what he or she wants to reveal or not, making privacy "a trade-off between protecting and sharing personal data"[27].

Consent is, at first sight, an appropriate response to this complexity and the requirement of a person's freedom in the use of his or her personal data: each individual is asked to accept or refuse a situation according to his or her individual and contextual interests. In so doing, it is accepted that he or she will sometimes consent to a legal situation that may cause him or her harm.

Consent is not a concept specific to data and privacy. It is also very common in the medical sphere: to preserve a patient's integrity, the doctor must inform his patient about any risks and obtain his consent for medical procedures.

BUT THIS APPROACH HAS ITS LIMITS

As we have shown, **consent**, as it is presented to the internet user today, is **neither pleasant, free nor informed**. It places the burden of ex ante arbitration on the individual alone, who has only limited information on the extent of the collection or on the uses made of his or her data, without any real choice or information. Improving it through the proposals we have already made is crucial, but so is questioning its relevance to all data-sharing situations on its own.

On the one hand, power is unbalanced between the individual and the companies requesting consent, which often have significant technological and economic power. Recourse to individual consent should not exclude the possibility of collectively prohibiting or regulating certain practices because they are considered to be harmful or of too limited interest to the individual or society. In the medical world, if consent is a prerequisite for any medical procedure, it does not exclude the supervision of practices through the prohibition of certain procedures and their control by competent authorities. In labour law, the contract concluded by employers and employees cannot derogate from the higher rules of labour law or collective agreements, which protect the employee and regulate the employer's practices.

The GDPR, with its twofold objective (to regulate data controllers and to confer rights on individuals), also responds to this logic but, voluntarily guaranteeing the free circulation of data, does not explicitly define constraints for, for example, the types of data controller, the

[24] *So complex that taxonomies are made of them! See Solove, A taxonomy of privacy.*
[25] *Nissbaum, H. Privacy in context, https://www.sup.org/books/title/?id=8862*
[26] *Warren, Brandeis, The Right to Privacy, Harvard Law Reviez, 1884.*
[27] *« Privacy as trade-offs arising from protecting [as opposed to] sharing of personal data". See Acquisti, Taylor and Wagman, The Economics of Privacy, 2016, Journal of Economic Literature, Vol. 54, No. 2, pp. 442–492.*

purposes pursued or the data collected[28]. **Recourse to individual consent should not exclude the possibility of collectively prohibiting or regulating certain practices** because they are considered to be harmful or of too limited interest to the individual or society.

On the other hand, consent is a highly individual notion: it betrays an individualised, even individualistic, approach, which contracts the relationship between a company and each citizen taken in isolation, in the name of personal freedom. In addition to the imbalance in power between an individual and companies, this individual character of consent effectively **excludes the collective dimension of data**. This collective dimension is a fact and concealing it can be detrimental to individuals and society: the value of personal data is increased tenfold by their networking and decisions taken by one individual have an impact on the data of other individuals[29] and have externalities on all individuals.

MOVING FROM THE INDIVIDUAL TO THE COLLECTIVE

In our view, in order to better control the collection, sharing and use of data, we urgently need to consider personal data issues as a political and collective problem, which is not limited to individual consent.

In order to place more emphasis on the collective dimension of personal data, we do not propose changing the GDPR, as this would involve large legislative changes and would not be a priority on the European agenda. Rather, we propose a change in approach. Individual consent ex ante and individual rights ex post can be enriched with new forms of collective action and collective choice.

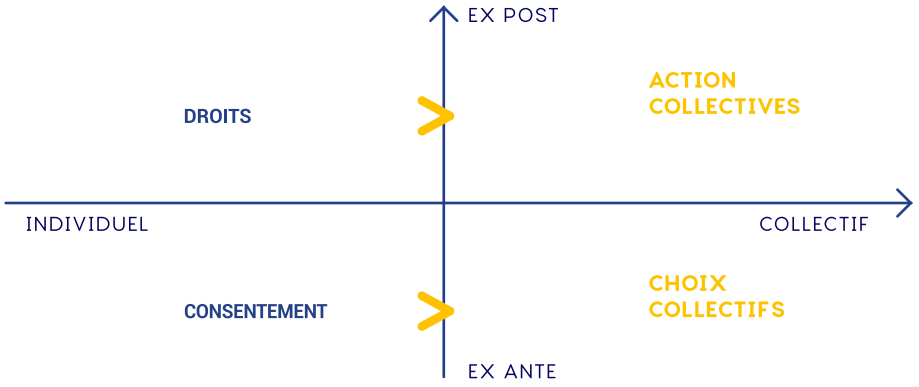


Figure 8 : Complementing individual consent and rights with collective action and choice.

CREATING THE CONDITIONS FOR COLLECTIVE ACTION EX POST

Individual ex ante consent and the trust it implies in the controller cannot exclude control. This is currently carried out by the regulator and we have already sketched out a few ways of strengthening it. However, beyond the regulator's action alone, we believe that the control action could be strengthened quantitatively and qualitatively by creating the conditions for inspection by civil society. This involves improving the exercise of individual rights, as mentioned above, but could be supplemented by the obligation to allow easy export of an individual recommendation thread or research result. This could eventually create the conditions

[28] *With the exception, in Article 9, of personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning the sex life or sexual orientation of a natural person are prohibited".*

[29] *For an economic definition: Acemoglu et al, online.*

for the regulation of algorithms by society itself, by associations from civil society or by the research world. An experiment of this type is being carried out by Media The Markup, which is highlighting biases by matching the recommendations made by Facebook to different users with their ethnic origin or political opinions.

Civil society action could also be facilitated by strengthening the provisions of group action, which could be made more easily accessible. At present, only three associations have the right to take legal action on personal data issues, leading to a bandwidth problem for the actions they are likely to take.

MAKING COLLECTIVE CHOICES EX ANTE

While the development of the internet was largely based on citizens' initiatives and associations, such as W3C, citizens and their representatives are today too little involved in its governance, and a fortiori in that of personal data.

We believe that there is a need to increase the participation of civil society, for example in institutions such as the *Conseil National du Numérique* and the CNIL. This could also be envisaged in structuring platforms through stakeholder committees; in the wake of the DMA and DSA, which recognise the systemic influence of these actors, on the market as well as on democratic issues, we could envisage involving citizens more strongly in their governance, to bring them closer to "common goods". For example, citizens could be more involved in the development of UGCs, in technical decisions, as well as in the definition of guidelines for the collection, processing and use of personal data.

A political and collective problem must first and foremost go through a democratic debate. This debate took place in consultations prior to the Law for a Digital Republic[30] or the entry into force of the GDPR and its media fallout, and it would gain from being extended. This can be done via ad hoc parliamentary committees, but also, in line with the experiments in the environmental field, via a citizen consultation on the digital environment, or even by a referendum. All of these solutions require strong political support, which is currently difficult to find, despite the consequences it has for public freedom, security and access to information.

[30] *https://www.data.gouv.fr/fr/datasets/consultation-sur-le-projet-de-loi-republique-numerique/*

SHOULD THE EXTERNALITIES OF TARGETED ADVERTISING BE LEFT TO THE SOLE CONSENT OF INTERNET USERS OR BE THE SUBJECT OF REAL COLLECTIVE CHOICES?"

V. EXAMPLES: WHICH OBJECTS FOR COLLECTIVE CHOICES?

In this section we look at two applications that can be used as concrete examples to illustrate collective choices.

The framework for general interest data provides an example of the articulation between individual consent, collective action and collective choices regarding data sharing. This articulation is not operative for data sharing in the targeted advertising sector, which relies heavily on individual consent, and this has very profound consequences for press publishers.

EXAMPLE 1: GENERAL INTEREST DATA

The health crisis has reopened the debate on the use of data from private companies by public authorities and for the general interest. Many have expressed regret that we could not follow Korea's example of accurately tracking the movements of infected individuals to verify their compliance with isolation, thereby controlling the COVID-19 outbreak more quickly. There are many reasons for the difference in solutions, but here we focus on the framework that allows for the **use of private data by the government.**

General interest data was introduced in France by the Law for a Digital Republic[31], without having any real normative scope outside companies delegating a public service. The law nevertheless provides for the use of certain data from the private sector by public authorities on a case-by-case basis and in a sectoral approach: mobility data, housing data, etc.

The report, resulting from the mission entrusted to MP Eric Bothorel[32], reaffirms the need to more clearly define this general interest data, particularly in cases where public authorities are not in a position to produce data of the same quality as the private sector, and to outline a doctrine for this general interest data. He emphasised the interest that digital traces or bank transaction data can have for monitoring health restrictions, as was the case in Korea, and recalled that some companies are already conducting partnerships by sharing aggregated data for research, regulation or public policy development.

In principle, the performance of a public interest mission is one of the six legal bases for processing[33] under the GDPR. A private company is therefore not required to obtain the user's consent to share public interest data with public authorities.

Nevertheless, the Bothorel report recommends using consent "in a logic of informational self-determination", a factor of social acceptability of the sharing of data of general interest. The Data Governance Act even introduces the notion of "**data altruism**", which will allow individuals (but also companies) to give their consent for the sharing of their personal data. This sharing can be done directly with the public authorities, but can also be intermediated by a trusted third party. This solution, which both the Digital Governance Act and the Bothorel report believe will help to overcome mistrust of the State, can go further and become the basis of "data commons".

In our view, **the use of consent in the context of public interest data is a good thing**, even

[31] *https://www.economie.gouv.fr/republique-numerique-ouverture-donnees-d-interet-general*
[32] *Bothorel E., Pour une politique publique de la donnée, 2020. The conclusions are based in particular on a consultation on acceptable uses of data of general interest.*
[33] *In Article 6 GDPR*

though a Senate report advocates the collection of health data in times of crisis[34] without mentioning consent. However, the same questions arise as in the case of data sharing between private companies: consent will be no less misused. We believe it is necessary to ensure that there is free and informed consent, but also clear alternatives.

Individual consent alone is not enough. The trust and good information of the citizen depend on the possibility for the latter to act ex post on this data and ex ante in the co-construction of solutions. It also requires the existence of a healthy debate and strong political support.

For us, these precautions are the only way to prevent abuse, to guarantee the trust of citizens, legal and reputational security for all actors and to make possible certain innovative applications in the exploitation of private data by public authorities.

EXAMPLE 2: TARGETED ADVERTISING

Targeted advertising is one of the strongest drivers of data collection, processing and use. It is therefore appropriate to question its impact and usefulness. Today, data sharing for targeted advertising is in the hands of the internet user. As we have shown, this request for consent is rarely free and informed, and is part of an unbalanced power struggle. For the user, being offered one product over another (and therefore more relevant ads) may reduce search costs and the number of ads they see, but these benefits must be weighed against the intrusive nature of some ads, which can be perceived very negatively.

For other economic actors, the usefulness also raises questions. Indeed, although the efficiency of targeted advertising is highlighted, its market price is currently up 4 to 5 times higher than contextual advertising. This value is shared between the (very) numerous players in the programmatic chain[35], but its distribution is questionable. The sector is dominated by a duopoly of Google and Facebook: these two companies alone control 75% of the French market. The record fine imposed on Google by the French Competition Authority also shows the existence of abuse of a dominant position[36].

All in all, AdTech is capturing most of the value to the detriment of content publishers, who are "seeing their advertising resources dry up, their relationship of dependence on platforms strengthen and their business models become more fragile"[37].

The report "Online advertising: for a level playing field", proposes various solutions to improve the sharing of value between players: aligning the legal framework of online display with that of television, activating brand safety to track ads, supporting the creation of unique identifiers, but above all, it proposes to act on market power (with proposals that are similar in many respects to the draft Digital Markets Act).

While this competitive aspect is essential, it cannot overshadow the issue of personal data. The sharing of this data is a fundamental element of online advertising and privacy issues must be taken into account in the organisation of a more desirable online advertising market. We have tried to formulate "pragmatic" solutions: supervision of the system of co-processors for targeted advertising, strengthening the application of the right of access.

The question of banning, or at least regulating, targeted advertising arises[38]: is it worth the risk? Should the externalities of targeted advertising, including the sharing of personal data and its consequences, be left to the sole consent of internet users or should they be the subject of genuine collective choices, specifying the conditions and accepting the consequences, if any?

[34] These senators propose the creation of a Crisis Data Hub, read online.
[35] The online advertising sector generated €5.1bn in revenues in 2019 in France, up 13% year-on-year. See Perrot, A., Emmerich, M., Publicité en ligne: pour un marché à armes égales, 2020, IGF.
[36] https://www.lemonde.fr/pixels/article/2021/06/07/publicite-en-ligne-l-autorite-de-la-concurrence-inflig e-a-google-une-amende-de-220-millions-d-euros_6083210_4408996.html
[37] Ibid.
[38] Lau Y., A Brief Primer on the Economics of Targeted Advertising, FTC Issue Paper, 2020, online.

NEWSPAPER PUBLISHERS WITHOUT TARGETED ADVERTISING?

These questions about targeted advertising can be examined in the light of their consequences for one area in particular: online content publishers and press sites. Indeed, today, many press titles are financed largely by targeted advertising: on average, 60% of press revenues are derived from digital, and of these, between 40 and 50% are derived from advertising (the rest from subscriptions)[39]. Making a choice on targeted advertising therefore has immediate consequences on the way online content publishers are financed.

Newspaper publishers are now the most fervent defenders of data collection. They are not the best pupils either: there is a very high number of co-contractors on their sites, some of them set up the famous cookie walls or find tools to secure data collection. For example, in reaction to the new CNIL guidelines and the suppression of third-party cookies (see Annex 3 of the report), six of them have launched a common identifier, the "Media Pass"[40], in order to continue collecting data for advertising in a logged environment, without depending on third-party cookies or too many consent banners.

The dependence on targeted advertising is also, as we have shown, a dependence on GAFAM and the world of AdTech, which capture a large part of advertising revenue. In order to reduce this dependency, many titles are defending subscription models, with or without cookie walls. While it is a guarantee of revenue, this model assumes an already acquired readership, which works for the major media (Le Monde, Les Echos) or independent media (Mediapart), and does not exclude broad data sharing.

However, the generalisation of subscription models leads to another problem: that of access to information. The predominance of a subscription model or one with cookie walls could make access to quality information more expensive, and thus pose a major democratic problem. It would also imply a strong shift in the current mode of information consumption by the younger generations, who are more likely to pick up information from various media, sometimes through a social network. The reduction in the number of sources available to each reader would increase the risk of information bubbles, a major issue at a time when the fight against fake news is becoming increasingly important in public policy.

Among the avenues currently being considered for financing the press, none seem fully convincing. Content aggregators are struggling to emerge except in niche markets such as students, due to the lack of agreement between the players and the lack of a market. The reforms of neighbouring rights currently being carried out, which aim to redirect part of the value captured by GAFAM to the online media, would make them financially dependent on these platforms, even more so than at present.

Consequently, replacing targeted individualised advertising with contextual advertising would lead to a drop in revenue from online advertising, which would have to be supported by the State, through various direct support mechanisms or the emergence of solutions such as aggregators. This is a major democratic issue: the independence of the national press in its sources of funding, particularly with regard to major foreign players, is an issue of sovereignty for the French and European media and a guarantee of the quality of democratic debate[41].

[39] *Figures from an interview with an AdTech player.*
[40] *Initiative under the umbrella of Geste, an association of publishers, read online.*
[41] *https://www.lopinion.fr/edition/international/guillaume-klossa-il-ne-peut-y-avoir-souverainete-politique -178529*

CONCLUSION

Our proposals aim to create the conditions in which the sharing of data by citizens can be carried out in confidence, by increasing their freedom of choice, the transparency of personal data use and by allowing democratic debate to shape it. Similarly to environmental protection, personal data protection is a collective problem and must be treated as such.

Our aim is not to sound the death knell for personal data sharing. The purpose of these proposals is not to generate friction that makes data sharing impossible, but rather to create socially-acceptable conditions for data sharing, which is necessary for the continuation of innovation related to personal data sharing in the long-term.

The good news is that the tools exist. By continuing the discussion around the GDPR, by improving its implementation, but also by daring to question certain practices, we can make the collection, processing and sharing of data more responsible.

WHAT DO WE PROPOSE IN THREE WORDS?

1. IMPROVE THE EFFECTIVENESS OF RIGHTS

by regulating the use of co-contractors for online advertising, by strengthening and facilitating the exercise of the right of access and by strengthening cooperation between European regulators.

2. MAKE CONSENT TRULY FREE AND INFORMED

by raising user awareness, improving the user experience, further regulating design and banning the cookie wall, and giving the user a real choice.

3. BETTER ARTICULATE CONSENT AND INDIVIDUAL RIGHTS WITH POLICY CHOICES AND COLLECTIVE ACTION:

by strengthening the provisions of group action, by restoring the place of civil society in regulation and digital companies.

OUR THANKS TO

This paper is the result of several months of investigation within the framework of our dissertation as mining engineers. It is also based on the joint report realized with the following students of the National School of Administration (ENA). We thank them warmly for the quality of the exchanges without which this work would not have been possible : Adrien, Quentin, Paul, Marie, Nicolas, Alexandre, Maximilien, Jenny, Camille, Arnaud, Aurélien, Shinya, Lena et Marie.

We would like to thank all the people who contributed and with whom we spoke. with whom we have spoken.

In particular, we would like to thank Pierre Fleckinger, professor of economics at the Ecole des Mines, for his important contribution and his unfailing support during all of this work.

Finally, we would like to thank the think-tank, and especially Axelle Lemaire and Arno Pons, for their Arno Pons, for their support in the publication of this paper.

DIGITAL NEW DEAL
THE NEW DEAL THINK-TANK

The aim of the Digital New Deal think tank is to shed as much light as possible on the changes taking place within the phenomenon of "digitalisation", in the broadest sense of the word, and to draw up concrete courses of action for French and European companies and public decision-makers. Supported by the expertise of its authors and their inclusion in the public debate, the think tank's work will be able to contribute to the development of French and European thinking on digital regulation in order to establish a balanced and sustainable framework.

THE BOARD OF DIRECTORS

The members of the Digital New Deal Board of Directors are all founding members. They come from various backgrounds while having direct contact with the digital transformation of companies and organisations. Given their shared interest in digital issues, they decided to deepen their debate by creating a formal framework for production and publication within which they can dedicate their complementary experience to serve public and political debate. They're personally involved in the life of Digital New Deal. Arno Pons, executive officer, is responsible for strategic steering with Olivier Sichel, founder and chairman, and supervises a project manager that coordinates all the think tank's daily activities.

SÉBASTIEN BAZIN
PDG AccorHotels

NATHALIE COLLIN
DG branche Grand Public et Numérique Groupe La Poste

NICOLAS DUFOURCQ
DG of Bpifrance

AXELLE LEMAIRE
Former Secretary of State for Digital Technology and Innovation

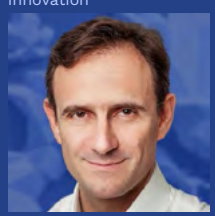
ALAIN MINC
President AM Conseil

DENIS OLIVENNES
DG Libération

YVES POILANE
DG Ionis Education Group

ARNO PONS
General Delegate of the Digital New Deal think tank

JUDITH ROCHFELD
Associate Professor of Law, Panthéon Sorbonne



OLIVIER SICHEL
President Digital New Deal
DGA Caisse des Dépôts

BRUNO SPORTISSE
PDG Inria

ROBERT ZARADER
PDG Bona fidé

OUR PUBLICATIONS

Fiscalité numérique, le match retour | Vincent Renoux - *September 2021*

Défendre l'état de droit à l'ère des plateformes | Denis Olivennes et Gilles Le Chatelier - *June 2021*

Cloud de confiance : un enjeu d'autonomie stratégique pour l'Europe | Laurence Houdeville et Arno Pons - *May 2021*

Livres blancs : Partage des données & tourisme | Fabernovel et Digital New Deal - *April 2021*

Personal data sharing: governance as a game changer | Matthias de Bièvre et Olivier Dion - *September 2020*

Reflections in the perspective of the European Digital Services Act | Liza Bellulo - *March 2020*

Préserver notre souveraineté éducative : soutenir l'EdTech française | Marie-Christine Levet - *November 2019*

Big Tech Regulation: Empowering the Many by Regulating A Few | Sébastien Soriano - *September 2019*

Sortir du syndrome de Stockholm numérique | Jean-Romain Lhomme - *October 2018*

Le Service Public Citoyen | Paul Duan - *June 2018*

L'âge du web décentralisé | Clément Jeanneau - *April 2018*

Fiscalité réelle pour un monde virtuel | Vincent Renoux - *September 2017*

Réguler le « numérique » | Joëlle Toledano - *May 2017*

Appel aux candidats à l'élection présidentielle pour un #PacteNumérique | *January 2017*

La santé face au tsunami des NBIC et aux plateformistes | Laurent Alexandre - *June 2016*

Quelle politique en matière de données personnelles ? | Judith Rochfeld - *September 2015*

Etat des lieux du numérique en Europe | Olivier Sichel - *July 2015*

contact@thedigitalnewdeal.org

thedigitalnewdeal.org

May 2022

thedigitalnewdeal.org