CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Autorité
de la concurrence

Competition and personal data: a common ambition

Joint declaration by the *Autorité de la concurrence* and the *Commission nationale de l'informatique et des libertés* (CNIL)

Tuesday, 12 December 2023

Introduction

How to turn consumer data protection into a competitive advantage? Can choosing to better protect your customers' personal data help to protect your market share? More generally, could anticompetitive practices be implemented under the guise of protecting privacy? These few questions illustrate the importance, for both companies and consumers alike, of the challenge of a right interplay between competition law and personal data protection. With the digital transformation of the economy, the importance of data in new business models, the growing role of large-scale digital platforms in our day-to-day lives and the race for innovation, this challenge is a practical issue for our fellow citizens.

The *Autorité de la concurrence* and the *Commission nationale de l'informatique et des libertés* (CNIL) have decided to address this issue together. The two authorities already have a long history of cooperation[1]. Given regulatory changes and practices in the field over the last few years, however, consideration is now needed on the next steps for a form of cooperation that can meet the new challenges. The CNIL and the *Autorité de la concurrence* intend to mobilise the synergies between their actions at the service of the users of the services concerned, who are both the consumers of these services and citizens with rights to the protection of their personal data. This mobilisation will also provide the economic stakeholders concerned with greater predictability and legal certainty.

This new, deeper form of cooperation between two independent authorities with distinct objectives consists, first and foremost, in developing a better understanding of each other, in order to improve the dialogue between the rules of law for which they are respectively responsible.

This declaration is a reflection of this common ambition. It illustrates the shared objective of the *Autorité de la concurrence* and the CNIL to reflect, together, upon how to take personal data protection and competition, respectively, into account in their actions. It defines the ways and means of cooperation between the two authorities, for the benefit of users and companies.

Based on this common ambition, this work will also help to identify common issues that may require further conceptualisation or analysis in the future.

[1] See, for example, the injunction issued by the *Autorité de la concurrence* against GDF Suez (now Engie) in 2014 (Decision 14-MC-02 of 9 September 2014 regarding a request for interim measures submitted by Direct Energie in the gas and electricity sectors). See also the Apple ATT decision (Decision 21-D-07 of 17 March 2021 regarding a request for interim measures (rejected)). The investigation into the merits of the case is ongoing.

The data economy: current issues, multiple regulations

The collection and use of consumer data are now central to the activities of many companies, which rely on this data to offer new services. Companies in all sectors of the economy are therefore developing strategies to access and exploit this data. The collection and use of personal data are already regulated, or are the subject of plans to do so[2], in a growing range of sectors (transport, finance, health, etc.), and this phenomenon is set to intensify, as illustrated by the recent adoption of the EU Data Act.

In this context, the interplay between competition law and personal data protection is the subject of particular attention. Some sectors are characterised by two-sided markets[3], bringing together users and professionals, or even multi-sided markets, bringing together more players, and, where applicable, by strong network effects (where the value of the service increases as the number of users increases). Certain platforms play a particularly structuring role in these markets[4], developing a range of interconnected services within integrated ecosystems, which can lead to the emergence of problematic practices in terms of both competition law and personal data protection.

France, Germany, the United Kingdom and the European Union[5]: a growing number of investigations and decisions concerning the practices of these platforms in terms of mergers or abuse of dominant position, but also the lawfulness of personal data processing, directly address these issues, which are at the intersection of competitive analysis and personal data protection.

Furthermore, several other regulatory frameworks, national provisions and European regulations, either already in place or are in the process of being adopted, may be applicable to this "data economy". Beyond the issues arising in connection with the implementation of competition law and personal data protection provisions in the strict sense, the very rich European regulatory data landscape[6] will necessarily lead to new interactions.

Innovative forums for exchange are emerging, such as the High-Level Group set up as part of the EU Digital Markets Act (DMA), which brings together networks of European regulators[7] to provide the European Commission with technical expertise and recommendations on the interactions between the DMA and other

[2] EU Data Governance Act, Digital Markets Act and Data Act.
[3] Intermediary such as a platform bringing together two types of clientele, supply and demand, that interact with each other for a product or service (e.g. advertising-financed media).
[4] For example, the European Commission has designated Alphabet, Apple, Meta, Amazon, ByteDance, Samsung and Microsoft as gatekeepers within the meaning of the Digital Markets Act.
[5] German *Bundeskartellamt*, 5 October 2023, Google case, B7-70/21; UK Competition and Markets Authority, 3 November 2023, Meta case, AT 51013 (commitments); *Autorité de la concurrence*, Apple ATT, Decision 21-D-07 of 17 March 2021 regarding a request for interim measures; European Commission, case M.9660, Google/Fitbit, 17 December 2020.
[6] EU Data Governance Act, Digital Markets Act and Data Act.
[7] European Competition Network (ECN), European Data Protection Board (EDPB), Body of European Regulators for Electronic Communications (BEREC), Consumer Protection Cooperation (CPC) Network and European Regulators Group for Audiovisual Media Services (ERGA).

relevant sector-specific regulations, of which there are many and whose interplay is complex.

The regulators and authorities concerned must therefore strive, at both the national and European levels, to establish the best interplay between the various applicable provisions. Their cooperation in that regard shall be commensurate with the issues at stake and rely on a fine-tuned governance of the implementation of their regulatory frameworks. The CNIL and the *Autorité de la concurrence* will therefore remain particularly attentive to the consistency of their cooperation at national level and with international developments and initiatives on these issues, particularly at the European level.

Privacy protection: a need for regulation, a parameter of competitive stimulation in the markets

From an economic point of view, the *Autorité de la concurrence* and the CNIL operate in a market economy based on the principles of consumer freedom of choice and entrepreneurial freedom. Free and undistorted competition helps to avoid rent-seeking behaviour that harms consumers. However, consumers – who make economic choices in a market – are also "data subjects" within the meaning of data protection, whose "informational self-determination" is protected by the GDPR.

The decision-making practice of competition authorities has evolved in recent years towards the recognition of personal data protection as a parameter of competition[8]. The level of personal data protection is therefore a parameter of quality that users take into account when making their consumption choices[9]. The maintenance of effective competition in the markets therefore favours, under certain conditions, the protection of personal data. Satisfactory competitive pressure is likely to encourage innovations promoting better data protection, which is valued by users, such as the creation of tools giving them greater control over their data.

Effective competition also encourages companies to differentiate themselves by proposing a variety of offers[10] (e.g. non-personalised offers that may have to be paid for), including offers with greater user privacy protection than their competitors.

[8] European Commission, case COMP/M.8124, Microsoft/LinkedIn, 6 December 2016; European General Court, 14 September 2022, Google and Alphabet (Google Android), case T-604/18, point 578; Opinion 18-A-03 on data processing in the online advertising sector, 6 March 2018, p.38 and p.112; Decision 22-D-12 of 16 June 2022 regarding practices implemented in the online advertising sector, paragraph 247.

[9] A decision-making factor, among others (e.g. price or functionality of the good or service).

[10] In addition to the "personal data protection" parameter, consumers will consider other product features (price, functionality, etc.), and may also have heterogeneous privacy preferences. In this context, and in a scenario of effective competition, companies should be required to propose several offers, with varying levels of protection for users' personal data.

However, the authorities need to take into account in their analyses the factors affecting competition in this regard, which are detailed below. Firstly, these factors may relate to market structure. Next, they may concern user bias and corporate behaviour, which influence users' reasoning abilities. Lastly, market failure phenomena need to be taken into account, such as actions that are detrimental or beneficial to the welfare of users or other economic agents, without any financial compensation for such changes in welfare (positive or negative externalities).

Firstly, consideration should be given to the specific structure of markets in the digital sector, which is marked by players with significant market power. Several digital markets are characterised by a trend towards concentration around platforms with structuring power, whose position is difficult for competitors to challenge. A strong potential for reducing service costs (economies of scale and scope[11]) and increasing their value (network effects[12]), sometimes backed by anticompetitive practices, makes these markets prone to "tipping" in favour of a single platform, while reinforcing the barriers to entry.

In the platform economy, business models based on the accumulation and combination of data are developing, and this accumulated data can represent a competitive advantage for the players involved. In certain cases, network effects specific to digital technology can lead to dominant positions being locked-in, with the risk of damaging competition and, at the same time, encouraging the misuse of personal data.

In these markets, demand is characterised by both a very large number of users and the limited individual capacity of these users to impact the functioning of the market. Their bargaining power is therefore insufficient in the face of well-established players with significant market power. For these reasons, users may, despite their sensitiveness to the protection of their personal data, forgo a comparable offer that is more respectful of their privacy.

Secondly, user behaviour can in some cases be influenced by the significant information asymmetry between users of digital services and companies in the sector, and by certain factors altering individual rationality, such as the influence of the context in which a choice is made, or possible consent biases (dark patterns, pre-selection of choices, etc.) that reduce consumers' freedom of choice. Understanding the interfaces, products, services and, more generally, the business models of the companies concerned, and their impact on consumer reaction, is therefore a key step in the authorities' analysis.

[11] Economies of scale: where an increase in production volumes leads to a drop in unit production costs due to fixed costs. Economies of scope: where a company reduces its production costs by expanding its range of products and services.
[12] Network effect: where the use of a good or service by new users increases the value of this same good or service for existing users.

Reducing information asymmetries is essential to encourage consumers to take into account the level of protection of their personal data, as a factor likely to influence their choice between different services or offers on the same market.

Lastly, understanding the level of personal data protection as a parameter of user choice means taking into account both the positive and negative externalities resulting from the collection and processing of this data (e.g. a cost borne by users or other economic agents resulting from the indirect provision of their data without their knowledge).

The two authorities therefore need, firstly, to correctly understand and, then, to minimise the effects of these unfavourable factors and, lastly, to actively promote virtuous competition supporting better protection of personal data. For example, they must ensure that dominant players do not abuse their position by reducing personal data protection in order to improve their revenues through the ever-increasing collection of information on their users. They must also ensure that the tools and procedures used by these players for the purpose of applying the GDPR take competitive risks into account.

The authorities can also work to guarantee better conditions for consumers to make free choices in the market. Consumers having control over their data is part of this and can be facilitated, in particular, by the protection of individual rights – consent and opposition, for example. Lastly, the authorities encourage the diversity of the product and services offering, concerning the level of personal data protection offered, thereby enhancing consumers' freedom of choice by allowing them to express their preferences.

Distinct but compatible objectives, synergies to be harnessed

The *Autorité de la concurrence* and the CNIL have distinct public policy objectives. The personal data protection mission entrusted to the CNIL aims to protect users against any harmful collection and use of their data, particularly when using commercial goods or services. Competition policy aims to guarantee the conditions for free, undistorted competition between companies in the market, in the interests of consumers, by promoting innovation, diversity of supply and attractive prices. So, while the CNIL protects an individual right recognised by the EU Charter of Fundamental Rights, the *Autorité de la concurrence* protects free and undistorted competition between companies in the market.

These distinct objectives converge, however, in that they are implemented for the benefit of users/consumers.

Both authorities therefore have a responsibility to work together, assisting each other in the name of the principle of sincere cooperation, as recently reiterated

by the Court of Justice of the European Union (CJEU)[13], to both protect citizens, by guaranteeing respect for their fundamental rights in terms of personal data protection, and ensure consumer welfare, by guaranteeing the proper competitive functioning of the market.

Firstly, the interplay between regulatory frameworks in the analysis of private players' behaviour is central. In the platform economy, the link between the degree of market competition and the level of personal data protection is of crucial importance. The economic exploitation of personal data therefore combines competition- and data protection-related issues and justifies particularly close cooperation between the two authorities in order to take full advantage of existing regulatory synergies.

The CNIL and the *Autorité de la concurrence* must pay particular attention to the interplay between the two legal frameworks for which they are responsible, which sometimes go in different directions. Economic impact studies show that data protection is proportionally less onerous for the largest players in the market, due to economies of scale that are likely to dissuade new entrants, thus justifying a level of requirement proportionate to the risks posed. As such, the impact of privacy protection standards on the functioning of competition shall therefore be taken into account at the stage when these standards are developed, just as the objective of protecting privacy can be taken into account as part of the competitive analysis.

Here too, the two authorities are deepening their dialogue. To date, the *Autorité de la concurrence* has been able to benefit from the opinions issued by the CNIL on various issues relating to the application of privacy and personal data protection legislation raised, for example, in the "GDF Suez"[14] and "Apple ATT"[15] cases. In March 2023, the CNIL formally asked the *Autorité de la concurrence*, for the first time, for an opinion on draft recommendations on mobile applications, designed to clarify the obligations of the different players in this sector with regard to personal data protection regulations[16].

New questions also arise when certain market players decide at their own initiative to amend and strengthen their privacy protection policies beyond what is required by the regulations. Some privacy policies raise the question of the possible use of privacy arguments for anticompetitive purposes. Examining this type of case will allow the authorities to develop the most appropriate doctrine for the interplay of the two legal fields, by dialogue and step by step, responding to the issues at stake.

[13] CJEU, 4 July 2023, Meta Platforms and Others, case C-252/21.
[14] Decision 14-MC-02 of 9 September 2014 regarding a request for interim measures submitted by Direct Energie in the gas and electricity sectors.
[15] Decision 21-D-07 of 17 March 2021 regarding a request for interim measures (rejected). The investigation into the merits of the case is ongoing.
[16] Publication of these recommendations is scheduled for 2024.

This closer and more frequent cooperation also enables the two authorities to identify, in practice, any harm to competition originating in data protection, or any risks to personal data protection that may arise or increase as a result of competitive factors.

Lastly, strengthening this cooperation and the synergies between both institutions will help to develop predictability and consistency, fostering competition and acting as a deterrent to behaviour that is anticompetitive or harmful to privacy.

The benefits of CJEU judgement C-252/21 of 4 July 2023 for the organisation of cooperation between the two authorities

In this respect, the recent Meta v. *Bundeskartellamt*[17] ruling by the Court of Justice of the European Union (CJUE) is highly instructive. The Court began by recalling the current thinking on this issue. Competition authorities and data protection authorities perform different functions and pursue different objectives. Nevertheless, access to personal data and the possibility of processing this data have become a significant competitive factor between companies in the digital economy. Consequently, the two legal frameworks cannot be viewed and applied with complete autonomy.

While preserving the competences of each authority, the reciprocal use of concepts for the needs and from the perspective of the other authority leads to dialogue between regulators and concepts, that favours synergies and the prevention of regulatory inconsistencies. Following this dialogue, each authority therefore remains free to decide on the consequences to be drawn in its own law, thus enabling the development of an in-depth cooperation while respecting each other's respective competences.

The Court therefore ruled that a national competition authority may find an infringement of the GDPR for the sole purpose of determining the existence of an abuse of dominant position, thus confirming that there is no reason to object to personal data protection being taken into account within the scope of the competitive analysis. Similarly, in the case of a data controller in a dominant position, the Court ruled that the assessment of the validity of consent must take this specific position into account, given the resulting restriction on the user's freedom of choice. If the data controller fails to provide for separate consent for certain additional operations (e.g. targeted advertising), consent would be presumed invalid. This judgement is therefore illustrative of the use that a data protection authority could make of a concept – in this case, the notion of dominant position – which relates to competitive market analysis.

[17] CJEU, 4 July 2023, Meta Platforms Inc. and Others v. *Bundeskartellamt*, C-252/21.

Lastly, this judgment affirms the need for enhanced institutional cooperation between national authorities, in accordance with the principle of sincere cooperation. Authorities must support each other, not compromise each other's objectives and avoid divergences. They must seek each other's opinions and respond within a reasonable timeframe, with a view to cooperating when the topics and points of application of their regulations intersect.

While at the national level, the CNIL and the *Autorité de la concurrence* have a long history of cooperation, the Meta judgement establishes a useful legal framework for joint cooperation between competition authorities and personal data protection authorities across the European Union. In this respect, the authorities will continue to consult each other for opinions as and when needed as part of their assessments or qualifications relating to the other area of regulation.

Ways and means of better integrating "privacy" and "competition" into the respective actions of the two authorities

In the fight against anticompetitive practices, the competition authorities will need to continue their work on how to integrate the personal data dimension into their analyses, in conjunction with the personal data protection authorities. This work is carried out from the perspective of parameters of competition, as well as that of the establishment and consolidation of market power, i.e. the ability to influence prices to the detriment of consumer welfare, and of the understanding of corporate behaviour aimed at imposing conditions unfavourable to users for their own benefit (abusive operating practices), in connection with the processing of personal data.

Data is at the heart of new theories of harm in competition law. The Meta case[18] of the German competition authority, for example, illustrates the emergence of exploitative abuses concerning the conditions under which users' personal data is collected and processed[19].

There is also the question of the use of corrective measures or commitments whose aim is to maintain sufficient competition in the markets (remedies)[20]. Obligations to share data with competitors, or conversely obligations not to combine data (data siloing) or even not to use data for their holders, must

[18] Meta decision of the *Bundeskartellamt* of 6 February 2019, B6-22/16. A summary of the decision is available here.

[19] On 5 October 2023, on the basis of national law (Section 19a of the German Competition Act, GWB), the German competition authority also issued Decision B7-70/21 requiring Google to offer its users the possibility of giving free, specific and informed consent to the cross-processing of their data. This latest case is particularly innovative in that the German authority has made binding the commitments made by Google, which, in substance, extend certain DMA obligations relating to the processing of personal data to more than 25 Google services that are not currently covered by the European Commission's designation decision under the DMA. The press release is available here.

[20] This approach is equally applicable to anticompetitive practices (abuses and cartels), merger control and opinions.

continue to be drawn up, while ensuring compliance with personal data protection provisions.

As regards the imposition of portability and interoperability obligations – or commitments proposed by companies –, which can in some cases foster competition and limit the market power of certain structuring operators, the design of such measures must also take into account their technical feasibility and the risks in terms of security and confidentiality of personal data. Allowing a greater number of third parties to access a platform could entail risks of unintended use of personal data or breaches of data security. Here too, effective coordination is required on a case-by-case basis between the authorities concerned, to ensure that the objectives of all the areas of regulation affected are preserved under the chosen solution.

The discussions to be held on the interplay between the two areas of regulation must also apply to merger control. The role of personal data in merger control should be analysed from two angles.

Firstly, from the angle of the resulting market power: for example, when the merger would lead to an accumulation of data by one company that would be materially impossible or too costly for its competitors to replicate in the market.

Therefore, competition authorities are led to examine innovative issues, such as the definition of markets for which data is an essential input. In particular, they may need to assess efficiency gains, such as lower costs or the improved quality of the products and services offered to consumers, to justify a merger, when the combination of the merging parties' data would enable them to improve these products or services.

Secondly, from the angle of the competitive parameter: for example, in the Microsoft/LinkedIn decision (2016)[21], the Commission considered that privacy protection was an important parameter of quality in the professional social network market – and therefore a parameter of competition.

The level of personal data protection, and in particular the compliance of the various players concerned with GDPR, may therefore be required to play a role in merger analysis. In the same way, the effects of the planned transaction on the level of personal data protection can be taken into account.

Lastly, the emergence of economic sectors based on the intensive use of personal data calls for reflection on the design of commitments in the context of merger

[21] European Commission, case COMP/M.8124, Microsoft/LinkedIn, 6 December 2016, "*Privacy-related concerns as such do not fall within the scope of EU competition law but can be taken into account in the competition assessment to the extent that consumers see it as a significant factor of quality, and the merging parties compete with each other on this factor. In this instance, the Commission concluded that data privacy was an important parameter of competition between professional social networks on the market, which could have been negatively affected by the transaction.*"

control – in line with similar reflections in the field of anticompetitive practices –, given the particularities and complexities of data markets.

The use of behavioural remedies – i.e. commitments constraining a company's commercial or strategic behaviour –, which have until now been adopted to limit the effects linked to the creation of large databases, such as the use of data silos[22] or access obligations[23], will have to be carefully analysed to avoid the pitfalls of the excessive cost and complexity of their design and the monitoring of their implementation, if necessary by involving the expertise of personal data protection authorities.

The imposition of structural remedies, i.e. remedies that have an impact on market structure and not just on the behaviour of players[24], in markets based on the collection and use of data also poses new questions for regulators. For example, the transfer – or deletion – of data can be complicated from an operational point of view, again requiring appropriate recommendations from data protection authorities.

In addition, the characteristics of a product or service are likely to condition its compliance or non-compliance with competition and personal data protection policies. It is therefore essential for economic stakeholders to take into account privacy and personal data, as well as compliance with the competitive framework, by design of a product or service[25]. Such a joint compliance approach will encourage consumers to choose the best-performing companies in this regard, provided that they can make their choices in full knowledge of the facts.

In turn, the CNIL is aware of the competitive repercussions of its decisions when acting on a market. Its most important decisions are therefore preceded by an analysis of the players' market position. It strives to anticipate any unexpected effects of legal choices. The concept of relevant market can inform its analysis of use cases and processing purposes. Dominance can also be taken into account when assessing the amount of sanctions. Lastly, the CJEU has encouraged the CNIL to give dominant position a special role in the analysis of freedom of consent, as an indicator that contributes, alongside other factors, to the assessment of a manifest imbalance to the detriment of individuals (see judgement C-252/21), and the CNIL will take up this opportunity.

Furthermore, the CNIL will be able to draw on the analysis of the market position and the lack of competition in this market to assume a more asymmetrical regulatory approach, given the greater risks to individual rights

[22] European Commission, case COMP/M.9660, Google/Fitbit, 17 December 2020; case COMP/M.9564, LSEG/Refinitiv Business, 26 February 2021.
[23] Ibid.
[24] The aim of structural remedies is usually to guarantee competitive market structures through divestiture of business or certain assets to an appropriate buyer that is likely to act as a real competitor, or the elimination of capital ties between competitors (Merger Control Guidelines of the *Autorité de la concurrence*, 2020).
[25] For example, at the data protection impact assessment stage.

and freedoms that this could entail. In terms of sanctions, such risks could potentially constitute an aggravating factor.

How can cooperation between both authorities be deepened from an operational point of view?

The provisions of the French Commercial Code (*Code de commerce*) and of Article 15 of Law 2017-55 of 20 January 2017 on the general status of independent administrative authorities and independent public authorities[26] enable cooperation between the CNIL and the *Autorité de la concurrence* to take place within a formal framework, in the form of requests for opinion, or within an advisory or litigation framework[27]. To date, the *Autorité de la concurrence* and the CNIL have been able to implement these mechanisms in a number of cases[28] and undertake to continue to seek the expertise of the other authority when appropriate.

In addition to the existing legislative mechanisms, both authorities may consult each other on an informal basis, in particular as part of exploratory exchanges of views on a given issue, or to prepare a formal request. To this end, there is regular contact, particularly between the *Autorité de la concurrence*'s Investigation Services and the CNIL's Directorate for Legal Support.

To ensure that these consultation mechanisms are fully effective, the authority concerned will seek the opinion of the other authority as far upstream as possible, and take this opinion into account in its analysis.

More generally, both authorities undertake to work towards a better understanding of each other's regulatory frameworks, so that they are in a position to better identify issues requiring a joint approach.

With regard to forward-looking studies, the CNIL and the *Autorité de la concurrence* may undertake joint studies on topics of mutual interest and, in this context, may hold joint hearings or issue joint calls for contributions. This joint

[26] *"An independent administrative authority or an independent public authority may refer to another authority for an opinion on any matter falling within the latter's competence."*
[27] Article R. 463-9 of the French Commercial Code (*Code de commerce*) stipulates that, "The General Rapporteur shall forward to the administrative authorities listed in Appendix 4-6 of this Book any referral relating to sectors falling within their competence. These administrative authorities have a period of two months in which to submit any comments they may have; this period may be reduced by the General Rapporteur if urgency so requires. These comments are attached to the file."
[28] In this way, the *Autorité de la concurrence* has been able to benefit from the opinions issued by the CNIL on various issues relating to the application of privacy and personal data protection legislation raised, for example, in the "GDF Suez" case (Decision 14-MC-02 of 9 September 2014 regarding a request for interim measures submitted by Direct Energie in the gas and electricity sectors) or the "Apple ATT" case (Decision 21-D-07 of 17 March 2021 regarding a request for interim measures (rejected). The investigation into the merits of the case is ongoing). Similarly, the CNIL has formally asked the *Autorité de la concurrence* for an opinion on draft recommendations for mobile applications, designed to clarify the obligations of the different players in this sector with regard to protection of personal data regulations.

work could lead to the identification of new regulatory issues requiring the convergence of their actions.

The CNIL and the *Autorité de la concurrence* will also continue to nurture and promote concrete exchanges (training for departments on common issues, exchanges between economic teams, exchanges of human resources, etc.), to support a lively cooperation.

Lastly, the *Autorité de la concurrence* and the CNIL will meet periodically for seminars with a more analytical and exploratory dimension. These seminars will provide an opportunity for both authorities' teams to develop their analyses on topics of mutual interest, such as artificial intelligence and the Internet of Things, and to deepen their understanding of common regulatory issues.

***

This declaration is intended to lay the foundations for closer cooperation between the two regulators. The CNIL and the *Autorité de la concurrence* will continue this dialogue to capitalise on regulatory synergies, in conjunction with stakeholders and public authorities.

To this end, in conclusion, the *Autorité de la concurrence* and the CNIL undertake to work on three fronts: concepts (to develop a common grammar, both economic and legal), doctrine (soft law, sector-specific recommendations and best practices, in order to bring together their capacities for action) and, lastly, practical cases (submitted to them or taken up by them).

Cooperation between the two authorities could also fit into the broader national coordination network for the regulation of digital services, provided for in the French draft law "to secure and regulate the digital space".

Cooperation between competition authorities and data protection authorities must also be stepped up at the European level. The CNIL and the *Autorité de la concurrence* will explore together the possibilities for cooperation between national competition authorities gathered within the European Competition Network (ECN) on the one hand, and the European Data Protection Board (EDPB) on the other[29].

For the CNIL,
The President,

Marie-Laure Denis

For the *Autorité de la concurrence*,
The President,

Benoît Cœuré

[29] The EDPB recently set up a task force on the interplay between data protection, competition and consumer protection ("C&C").