The future ePrivacy regulation will reform the protection of privacy applied to electronic communications: telecommunications networks, messaging services, online tracking and geolocation. **La Quadrature du Net promotes seven clear positions for the protection of privacy.**

1. Adopting a Regulation specific to electronic communications

GDPR: a general Regulation applicable to all sectors

In spring 2016, the European Union adopted a General Data Protection Regulation (GDPR). As of the 25th of May 2018, this Regulation will apply to anyone processing personal data, whatever their sector: medical, banking, administrative, insurance, human resources, public services, on the Internet, etc.

On a number of points, the Regulation provides for rules common to all sectors (security obligations, data subject's rights, supervision by independent authorities, sanctions...). These rules are not challenged by the ePrivacy Regulation: they will continue to apply to electronic communications as such.

'Legitimate interest': a dangerous general exception

The GDPR had to respond to the following fundamental question: in which case is it acceptable to process personal data without data subject's consent?

In view of the diverse range of activities to which the GDPR applies, the European legislator has chosen not to draw up an exhaustive list of purposes allowing to bypass consent. Instead, a particularly uncertain solution has been chosen, a legacy of the 1995 Directive: each actor defines for himself, according to his field of activity, what 'legitimate interest' (a purpose producing benefits that outweigh the inconveniences it causes) may authorise him to process data without consent.

The danger of this solution comes from the fact that, in the first instance, **this balance is defined in a unilateral way by each actor, who is both judge and defendant**. It is only in the second instance, and in the rare cases in which it comes under examination, that Data Protection Authorities (DPAs) and judges are able to check this balance and to fine those who have not respected it.

An unjustifiable danger without sector-specific limitations

If the legislator has accepted such a dangerous solution, which is perfectly contrary to the objective of legal certainty, it is only because other European laws can then define, sector by sector, a **concrete and restrictive list of purposes which may allow to process personal data without consent**.

If the European Union were not to seize this opportunity to list as extensively as possible such purposes in major sectors of activity, the GDPR would contravene the most fundamental respect of personal data. Listing such purposes was the principal objective pursued by the the ePrivacy Directive and which this Regulation should pursue, too.

Precisions specific to electronic communications

Some of the general rules provided for by the GDPR need to be refined when they apply to electronic communications. A number of fundamental issues need to be resolved concerning, *inter alia*, how consent may be freely given on the Internet, who can consent to the processing of personal data concerning more than one data subject, or how data which have already been collected may be reused for State surveillance.

Such precisions are all the more important since electronic communications produce **data which are already structured**, making their automatised analysis particularly efficient at revealing an invidual's physical or emotional state, location, habits, opinions or social interactions.

Furthermore, the GDPR only protects the right to the protection of personal data enshrined in article 8 of the Charter of Fundamental Rights of the EU. The ePrivacy Regulation will also protect the respect for private and family life protected by article 7 of the Charter, which covers the confidentiality of electronic communications.

2. Limiting the exceptions to consent

Regarding electronic communications, the proposed ePrivacy Regulation defines the purposes which justify the processing of data without data subject's consent. These purposes can be summarised into three objectives: **the provision, the safeguarding, and the invoicing of services requested by users**. The list of these purposes is restrictive and exhaustive: any purpose that is not included in that list can only be pursued with users' consent.

'Legitimate interest' is unjustifiable

Some actors propose the integration of a 'legitimate interest' exemption in the ePrivacy Regulation. Such a proposal is contrary to the structure of the EU personal data law: the very aim of a sectoral law such as ePrivacy is precisely to restrict the risks of the 'legitimate interest' general exemption provided for by the general law (the GDPR).

Nonetheless, some actors know that the purposes they wish to pursue without consent (usually advertising purposes) will never be included in the 'list of lawful purposes' by the legislator. Therefore, rather than explicitly ask to include such purposes, they prefer to ask for the creation of a 'legitimate interest' exemption. The validity of such 'legitimate interests' being assessed only *a posteriori* and at the initiative of DPAs, these actors hope that, in practice, they will be able to bypass consent for purposes that the legislator would never have admitted.

Accepting this 'legitimate interest' exemption amounts to **admitting that the legislative debate might be entirely sidestepped** and to denying that the legislator should play any role.

'Further processing': an even more dangerous exemption

The GDPR provides (see art.6, paragraph 4 and recital 50) that data collected based on a 'legitimate interest', consent or any other legal grounds can be re-used without further consent, as long as this is for a purpose 'compatible' with the initial purpose for which they were collected.

This exception is inspired by the same logic as the 'legitimate interest' one: since the GDPR affects an infinity of different activities, the legislator has allowed an especially unpredictable and risky exception. For the same reason, such an exception cannot belong in a sectoral text which principal aim is to list the purposes allowing to process data without consent.

Furthermore, this exception is not even based on any balance of interests, but on the very vague notion of compatibility which, as defined by the GDPR, has **no proportionality criterion**. Moreover, here too, the compatibility is unilaterally assessed by those who benefit from it, who act as both judge and defendant again.

Pseudonymisation: just a security measure

Some actors wish to be able to process without consent and for any purpose any data which have been pseudonymized. Technically, pseudonymized data are a set of personal data spread among several distinct databases. This spread **does not prevent the cross-referencing of data at all**, but is just a security measure which aims, *inter alia*, to reduce the consequences of a data breach.

Pseudonymization is a sound measure that should be implemented whenever it can. But consent should never be bypassed simply because some security measures are implemented. **Personal data law has always based the lawfulness of processing on their purpose**, and never solely on their level of security. It should remain this way.

3. Protecting the freedom to consent

The GDPR specifies that '*consent is presumed not to be freely given (...) if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance*' (recital 43, clarifying art 7, paragraph 4).

If consent is given under the threat of a loss (the denial of access to a service, or the payment of money), it is invalid. Thus, **consent can never be the counterpart of a good or a service**. It is valid only if it concerns an operation requested by the user, or if it is given in a disinterested way.

Freedoms have no economical value

Admitting that consent could be an economic compensation would mean that fundamental freedoms may be attributed according to economic criteria. Privacy would become **a luxury affordable only to the 'happy few'**.

Outside the communications sector, some practices are typical examples for this. This includes loyalty cards, offered by big stores and that allow companies to establish detailed profiles from their customers' daily consumption, hence characterizing their sheer intimacy. Whereas the 'happy few' can afford to escape this surveillance by not using these cards, the poorest people often have no choice. Refusing to submit to such surveillance would deprive them from promotions often necessary to close their budget. They cannot afford the 'luxury' of privacy nor the 'ease' of not being under surveillance. However, such things are not luxury nor ease but fundamental freedoms.

For this reason, and to fight against such abuses, these fundamental freedoms have all been taken off the market: physical integrity (Art 3(2)(b) of the EU Charter prohibits the sale of one's own body parts), the freedom of decision over one's own body (Art 5 of the Charter prohibits submission to forced labour), the freedom to marry, to vote, etc. This should be no different when it comes to privacy and to the confidentiality of communications.

A business model opposed to information quality

Several websites claim they cannot let their users choose whether to accept targeted advertisements or not. Otherwise, these websites would presumably be unable to fund themselves and thus to provide their services. These claims are probably true for some websites (e.g. Facebook), but are definitely not correct for many others. In particular, press publishers have taken up this discourse, though it is contrary to their situation.

The business model of the press is traditionally based on sales and subscriptions. This model seeks to retain its readership by assuring that quality analysis and investigations are provided. This model is being grossly called into question by competitors providing simple and diverse entertainment and news for free, most of which requires a short reading time and targets the widest possible audience. This new business model relies only on **targeted advertisement, which revenue depends on the number of visitors and not on the quality of the provided information**.

The competition imposed by these new actors forces an important part of the traditional press to change their business model (not without pain) and the way in which the media produces information. For example, they invest more in sensationalist coverage and 'infotainment', and less in analysis and investigation.

This development will inevitably harm the quality of public debate, but it can be limited very easily by prohibiting sites from blocking access to users who refuse targeted advertisements. Such a measure to protect Internet users would present a strong challenge to the sort of business model founded on targeted advertisement and, with the swing of the pendulum, make the traditional models that rely on the quality of information and the fostering of the readership's loyalty much more viable. Above all, this protection would create lasting reconciliation between a sustainable business model for the press and respect for the fundamental rights of its readers.

Conceded consent is not freely given

Service providers must remember users' choice not to consent. They should not repeatedly ask the same person the same question over and over again, until he/she gives in. Such consent would otherwise not be freely given but obtained through harassment.

For example, on an Internet site, a banner inviting users to consent to use cookies should not reappear on each page of the site after the user has refused them once already. If not, many users, worn out by the constant inconvenience of the banner, would end up giving their consent in order to avoid enduring the continual annoyance. **A freely given consent may only be requested one time per Internet site.**

Technically, a solution for sites could be to deposit one simple cookie on the user's terminal. Such a cookie would be identical for all users and simply indicate 'cookie: no'.

4. Requiring comprehensive consent for communications analysis

Consent from all users

The proposed Regulation (article 6) provides that electronic communications can only be analysed for one of the listed purposes (conveyance, security or billing) or if the user consents to it.

Regarding communications, there are in principle several users: the sender and the recipient(s). However, the current draft Regulation generally requires the consent of only one of these users (whether it concerns the sender or one of the recipients is not specified). The Regulation should be modified to clearly require consent from all users. **A single user should not be able to consent in the place of others.** The ECHR has clearly stated that this would be a violation of the confidentiality of communications[1].

In the case of email, for example, a communication provider wishes to analyse a message's metadata in order to suggest targeted advertisements to its user (Gmail, typically[2]). It should have to obtain consent from its own user (registered on Gmail) as well as that of the exterior user (who is not registered) - by sending an email to the latter. If this exterior user refuses, the email service provider should have to respect his/her choice and not ask for his/her consent again (by registering a fingerprint of his/her address on a list, for example).

Finally, as an exception, there is only one case in which requiring the consent of the sender would lead to a breach of rights: the case of anti-spam. Here, only the receiver's consent should be required.

1 ECHR, *A c. France*, 23 november 1993, n° 14838/89: recording a call with the consent of only one caller is a breach of the right to confidentiality of communications of the other caller.

2 Gmail has stated that it will no longer process the content of email for advertising purposes but seems to keep processing metadata: https://www.blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align/

The same consent for all data

The draft Regulation requires (article 6) a different type of consent in order to analyse the content of electronic communications or their metadata (which cover the identity of the users, date and volume of the message, attachments...). The metadata require consent from only one of the users, while this requirement is variable and more ambiguous concerning content (article 6, par. 3).

This distinction makes no sense: both types of data should be protected in the same way. As the EU Court of Justice has recently emphasised[3], metadata are '*liable to allow very precise conclusions to be drawn concerning the private lives of the persons [...], such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (...). In particular, that data provides the means (...) of establishing a profile of the individuals concerned, **information that is no less sensitive, having regard to the right to privacy, than the actual content of communications***'.

5. Opposing automatic consent for tracking

The proposed regulation stipulates that users should be able to give their consent automatically to on-line tracking via the configuration of their communication softwares. For example, at the time when they install their Web browser, users should be able to accept in advance all future depositing of cookies.

This proposition is totally in opposition to the GDPR's requirement (art. 4, para. 11) that consent should be 'informed' and 'specific'. Thus, it must be rejected. Any consent given before the user even knows the controller, purpose and nature of the processing, or whether the data could be transfer outside of the EU, **can never be considered as being 'informed'**. Likewise, a unique choice concerning an infinite number of processing is completely **contradicting the definition of 'specific'**.

6. Requiring consent for geolocation

Concerning the geo-tracking of individuals based on data emitted by their devices, the European Commission has proposed several recitals that are incoherent with the proposed articles.

On one part, the data emitted by devices in order to connect to a network are considered as metadata that can never be analysed without consent (recitals 17 and 20). On the other part, data analysis is authorised for any purpose whatsoever and without consent (article 8).

The ePrivacy Directive had taken into account the significant danger raised by this practice by requiring quite explicitly users' consent to the analysis of such data (art. 6 and rec. 35). **The Regulation has no reason to reduce the protection of individuals' privacy.** In the cases where processing data emitted by devices may benefit the society as a whole, enough users would gladly give their consent. There is no need to bypass it.

Equally, it should not be possible to use emitted data to contact users on their devices in order to obtain their consent. That would amount to '**offline spamming**', a practice both unacceptable and incompatible with a freely given consent. The user should only be able to consent through a proactive action, by contacting the controller to give his/her consent (the controller can inform users of this possibility through notices displayed where the tracking ought to take place, for example).

7. Regulating State surveillance

Article 11 of the proposed Regulation allows Member States to authorise or to oblige service providers to collaborate with them in order to monitor users' activities and communications.

Contrary to the ePrivacy Directive, the proposal permits such surveillance for '*other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security*'. This extension is injustifiable.

Rather than extending the boundaries of State surveillance, it is essential that the ePrivacy Regulation **incorporates the decisive limitations recently laid down by the EU Court of Justice**[4].

The Regulation must prohibit service providers from engaging in mass retention of information concerning all of their users. The only acceptable restrictions of fundamental rights should be those than are necessary to fight against **serious crimes**, that are **authorised by a judge, limited in time** (two months regarding data retention) and **targeting identified individuals**.

3 CJEU, *Tele2* case, 21 dec. 2016, C-203/15 & C-698/15

4 CJEU, *Tele2* case.