ISTITUTO ITALIANO PER LA PRIVACY E LA VALORIZZAZIONE DEI DATI

PRIVACY NUTRITION LABELS VS. PRIVACY DYNAMIC TARGETING

Ex-ante and *ex-post* models for the administration of privacy information and the exercise of data subject rights

Luca Bolognini[1] - Marco Emanuele Carpenelli[2]

May 28, 2021

DOI 10.5281/zenodo.4836088

[1] L.Bolognini@istitutoprivacy.eu – President of the Italian Institute for Privacy and Data Valorisation
[2] M.Carpenelli@istitutoprivacy.eu – Fellow of the Italian Institute for Privacy and Data Valorisation

Abstract

While the static *ex-ante* model, like the one developed by Apple with the *Privacy Nutrition Labels*, is still anchored to traditional information administration criteria (even if in innovative and creative ways) and risks collateral effects on the free economic initiative and freedom of expression of developers, the dynamic *ex-post* model adopted by other operators seems to offer a clearer idea of the future of privacy. The algorithms in this sense could be the antidote to themselves.

Our proposal is to direct the potential of the use of algorithms, if developed in an intelligent way, toward different purposes with respect to those typically commercial or statistical, making the personalised profiling of data subjects more pro-privacy through a sort of behavioural targeting intended to favour greater uniformity in the experience of the various virtual spaces visited by browsers. This way, for example, if site x registers an objection to processing, this objection is also proposed in site y so as to ensure that the experience effectively and organically adheres to the privacy preferences expressed by the data subject.

We could define this kind of initiative as *Privacy Dynamic Targeting*: Apps and websites dynamically "follow" or, better, "accompany" data subjects, analysing their behaviour and recording their preferences (also) with the purpose of uniformly ensuring their informational self-determination in each of the digital scenarios they encounter. The effect in these cases would be that of systematically and coherently personalising the privacy-information experience to the advantage of the data subjects. By exploiting algorithms as an antidote to algorithms, *Privacy Dynamic Targeting* would give rise to a type of personal data processing that could well find its roots in the legitimate interest of the controller and interested third parties as per article 6 (1)(f) of the GDPR.

By abandoning the concept of the privacy information notice as a singular, static summary of information on the processing of personal data (as we find in nutrition labels, or, continuing the metaphor, in a static menu abstractly describing ingredients and dishes), the dynamic *ex-post* model disaggregates the information and releases it precisely in the digital spaces where the processing effectively takes place (as would be the case, continuing the nutritional metaphor, of a waiter describing the qualities and characteristics of the dishes as they're being served, in real time). In the future, the dynamic *ex-post* model could evolve further and develop in at least two directions. One could involve the use of algorithms not already serving typically commercial or statistical purposes, for profiling data subjects according to the privacy preferences expressed in the various digital spaces they visit, thereby ensuring uniformity in their digital self-determination. This corresponds to the *Privacy Dynamic Targeting*. The other could involve combining the information functions with the functions for the exercise of the rights provided for under articles 15-22 of the GDPR, which could finally turn the concept of privacy into something live and interactive.

1. Transparency and *accountability*: the privacy information obligations of data controllers

«*Personal data shall be* [...] *processed* [...] *in a transparent manner* [...]»: with these words, article 5(1)(a) of (EU) Regulation 2016/679 (the "GDPR") establishes the principle of transparency and reflects the more general need to ensure data subjects clear and accessible information on the processing of their personal data. The principle is primarily expressed in articles 12, 13 and 14 of the GDPR through a series of regulatory provisions that impose more specific obligations on data controllers in terms of the formal profile and content of the information, as well as the procedures and timing for its issue to data subjects.

The provisions of article 12 detail the formal and procedural requirements for administering the information. They require data controllers to take "*appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.*" (art. 12 (1) of the GDPR).

In terms of the administration procedure, the information may be provided "*in writing, or by other means, including, where appropriate, by electronic means*" or even "*orally*", when requested by the data subject, provided that the identity of the data subject is proven by other means, in compliance with the more general need for *accountability* (art. 12(1) of the GDPR); the provisions establish that information may also be provided "*in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing*", with the specification that if "*the icons are presented electronically they shall be machine-readable*" (art. 12(7) of the GDPR). To this regard, *Recital* 58 of the GDPR adds that "*This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal*

data relating to him or her are being collected, such as in the case of online advertising".

On the other hand, articles 13 and 14 of the GDPR establish the content requirements and terms for providing privacy information, distinguishing between cases where personal data is collected directly from the data subject, and cases where the data is collected from other sources. In the former case, data controllers have to provide the information required by article 13 "*at the time when personal data are obtained,*" (art. 13 (1) of the GDPR); on the other hand, in the latter case the obligation concerns the information required by article 14, which includes specific indication of the source of the data, and which must be fulfilled either "*(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed; (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.*" (art. 14 (3) of the GDPR).

In practise, the methods for complying with these obligations are left to the *accountability*, creativity and expressive originality of the data controller (art. 5 (2) of the GDPR). As such, *accountability* offers a unique opportunity for selecting and personalising the information to provide to data subjects[3]. More specifically regarding the methods for administering the information, the data controller is free to choose how to call the attention of data subjects browsing the *web*, how to involve them in reading the information displayed on-screen and how to ensure that they understand it; above all, the data controller is free to choose whether to allow them to effectively control the frenetic flows of the personal data concerning them, and, in doing so, make sure that privacy doesn't simply become a mass of *pixels* destined to dissipate following an absent-minded *click* on the "*accept and continue*" button.

[3] On this subject, in a communication dated 15 March 2021, the Italian Data Protection Authority launched a contest entitled *"Easy privacy information via icons? Yes you can" The Supervisory Authority calls on collective creativity*, for solutions to make sure information notices "*that are really helpful and suitable for the purpose for which they are intended*".

2. Practises and models for administering privacy information

In the current scenario, the practises of the leading companies on the market are moving in original directions, little explored until recently. We are seeing the gradual development of two distinct and opposing models for administering the information required under articles 13 and 14 of the GDPR, in graphic and in any case simplified and "user friendly" form: one a static *ex-ante* model, akin to the policies of Apple for example, and the alternative that is a dynamic *ex- post* model, attributable to the practises usually adopted by other Over The Top players.

2.1. The "static *ex-ante* model"

Since December 2020, with the appreciable aim of ensuring better and more uniform quality in the information provided to developers interested in publishing their products on the App Store, Apple requires that they comply with precise and mandatory contractual obligations[4]. In effect, it was often found that the information provided to developers didn't meet the standards required by the applicable norms; in some cases the *links* weren't even working.

On the contrary, now the developers are under a contractual obligation (further to those imposed under articles 13 and 14 of the GDPR) to comply with a series of preliminary requirements. Now, to publish *apps* and updates on the *App Store* developers have to identify the personal data collected and processed by the developers themselves or by third parties, and categorise it according to the types indicated by Apple (the most significant of which being "*Contact Info*", "*Health and Fitness*", "*Location*", "*Sensitive Info*" and "*Usage date*"); then they have to identify the purposes of the processing, distinguishing between those purely commercial ("*Third Party advertising*" and "*Developer's Advertising or Marketing*"), those for statistical analysis ("*Analytics*"), those strictly related to the functionality of the *app* or aimed at improving the usage experience of the *app* itself ("*Product Personalization*" and "*App*

[4] See https://developer.apple.com/app-store/app-privacy-details/#data-type (last acc. 2021/05/28).

Functionality") and all the others ("*Other Purposes*"); particular attention is given to identifying any tracking activities ("*Tracking*"), understood as operations that combine data on users or their devices, collected by the *app* itself (for example, *user ID*, *profile ID*, other profiles), with other information available to third parties for targeted advertising purposes, or other ways of valorising the information pool, such as transferring data to *data brokers*.

All of the above information has to be filed in the virtual folders displayed to *App Store* users in the area around the "*download*" key. Apple has called these virtual folders *Privacy Nutrition Labels*[5] in an amusing metaphorical reference to the labels on the backs of grocery products[6]. These are essentially tables labelled with captivating icons offering users a graphic summary of the information pertinent to personal data protection. *Correction*: a graphic summary of the information that Apple considers pertinent. Because as we have seen, it is Apple that decides what information is worth presenting to users, and again Apple that decides how to present it, by imposing mandatory compliance with the *Privacy Nutrition Labels*. The only margin of decisional autonomy reserved for developers regards so-called "*Optional disclosure*", by which in certain conditions Apple allows developers to omit some information on the processing of the data, which would - plausibly - be included in the full text of the privacy notice provided by the developers later in the scope of the *app*, in compliance with the regulatory requirements.

As for the rest of it, despite the admirable intent of strengthening the guarantee of processing transparency, the rules imposed by Apple risk binding companies into rigid compliance with pre-set models for administering information - or better, of only certain data - with enormous impact on the market in terms of limitations to the freedom of choice of other data controllers. Not only that: Apple's hegemony can also

[5] In further metaphorical reference, L. BOLOGNINI, Artificial Insanity. *Reflections on the resilience of human intelligence*, 2018, ISBN 8849859996, pp. 64 and 65, in which the author imagined similar solutions, defining them as "snack labels".

[6] Among the studies which have dealt with this subject, in the last years:

- Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, Robert W. Reeder, "A "nutrition label" for privacy", Publication: SOUPS '09: Proceedings of the 5th Symposium on Usable Privacy and SecurityJuly 2009 Article No.: 4 Pages 1–12 https://doi.org/10.1145/1572532.1572538
- P. Emami-Naeini, Y. Agarwal, L. Faith Cranor and H. Hibshi, "Ask the Experts: What Should Be on an IoT Privacy and Security Label?" in 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, US, 2020 pp. 447-464. https://doi.ieeecomputersociety.org/10.1109/SP40000.2020.00043

be revealed considering that, in the event of interpretative differences in the qualification of a given element relevant for privacy purposes, the solution advanced by Apple will in fact always prevail over the interpretative reconstructions of the developers. Thus, for example, if Apple systematically tends to believe that a certain processing activity constitutes online tracking and therefore falls into the aforementioned category of "Tracking", it will be very likely that, even where the developer disagrees, in the nutritional labels we will find Apple supported qualification indicated. Arriving in this way to bend and sacrifice the free hermeneutic initiative of developers, Apple's categorizations could gradually allow interpretative guidelines to settle into practice to which developers could have no choice but obey; this would in fact allow Apple to unilaterally model the data protection designers' conceptual schemes and tools, even the most controversial and debated ones. In other words, passing through the definition of language, Apple's influence could end up determining various and notable alterations of the conceptual perimeter and of the very meaning of the categories relating to the protection of personal data, as generally conceived by the community of professionals in the field: in this sense, to take the example above, the concept of online tracking could thus be destined to universally overlap the concept of "Tracking" defined by Apple.
In this way the establishment of contractual obligations over and above those established by law risks to create abnormal interference in the *accountability* and freedom of expression of developers, as independent data controllers, and risks obstructing their free economic initiative.

Above all, the policies adopted by Apple, although with the best of intentions, risk discouraging and slowing the multiform development of innovative and original solutions for administering privacy information, often a determining factor in ensuring the effective utility of the information on personal data processing. In effect, despite their clear and intuitive graphics, the *Privacy Nutrition Labels* overwhelm data subjects with a multiplicity of *input* information not easy to grasp, understand and contextualise in the real experience of using the *app*. It is easy to imagine that most data subjects would simply scroll through pages just to get to the *app download* quicker, without even bothering to read them.

The point is that with *Privacy Nutrition Labels*, data controllers simply provide data subjects with a static summary of the same information given in more detail in the full text of their privacy information notices; an outline of the information concerning the processing of their data; a panorama of a landscape whose details are difficult to distinguish with the naked eye, details like not being able to foresee the concrete consequences of the use of their data in future scenarios[7].

These are the reasons why the Apple model is defined as a "static *ex-ante* model": the information remains static within a pre-set framework, provided to data subjects before data processing takes place effectively in its concrete, dynamic manifestations; moreover, while aiming to provide a schematic overview of a great deal of complex information, the Apple model meets an inevitable compromise, that of never really entering into the precise details of the information itself.

So, in most cases, *Privacy Nutrition Labels* remain suspended on a white background, without any concrete connection to the real application, easily forgettable and ignored by the data subjects.

[7] Moreover, with the *ex ante* approach, what is indicated in the Privacy Nutrition Labels does not always accurately reflect the peculiarities of the experience that the data subject will choose to have in interacting with the app. Thus, for example, if an app offers functions based on the user's geolocation - and the subject is made aware of this function through the relative Privacy Nutrition Label -, since the user is required to opt separately for this kind of functions (*id est*, through specific and distinct authorization to access geolocation data), the inclusion of geolocation in the Privacy Nutrition Label may be irrelevant for the subset of users who choose not to use this functionality.

2.2. The "dynamic *ex-post* model"

Trying out solutions different to those chosen by Apple, other large corporations, usually OTTs, seem to be taking different approaches to the administration of information on personal data processing. Both models have the same goal - that of ensuring effective accessibility and a real understanding of the information provided - but in this case the strategic design approach seems more dynamic and attentive to the real consequences of the processing itself.

In particular, rather than being limited to gathering the pertinent information in tables and graphic summaries, like *Privacy Nutrition Labels*, this approach tends to favour a more fragmented administration of the information, to be provided when required at the moment the processing effectively takes place. This could be achieved in concrete terms using *pop-up* information *banners* or introducing special "*privacy*" keys to click on. In this way, information pertinent to a particular service offered by a *web* platform would be provided to the data subjects only if and when they decide to use it[8]. Thus, for example, many will have happened, shaking the Facebook home, to ask themselves the reason for viewing a certain advertisement; offering the interested party an easy and immediate possibility to find out and implement any necessary and consequent updating of privacy preferences, Facebook makes the "Why am I seeing this?" option available. Still, others will have noticed that, by setting the address of their home in Google Maps, the app draws the attention of the interested party to the fact that, except for his/her opt out, the information provided will also be used in the context of the other Google apps.

Of course, even in this scenario, the issue of the information *ex-post* and downstream does not entirely substitute the provision of a more formal, organic and complete text *ex ante* and upstream, containing all the information required (according to case) by article 13 or article 14 of the GDPR.

[8] Cf. again L. BOLOGNINI, Artificial insanity. *Reflections on the resilience of human intelligence*, 2018, pp. 64 and 65.

The dynamic *ex-post* model thus breaks with the static nature of solutions like *Privacy Nutrition Labels*, replacing the *a priori* summary approach with a more agile and dynamic solution that meters out the information throughout the different and disaggregated phases of the processing, informing data subjects in a more analytical way about the purposes of processing, the data processed, the recipients and other elements that are only significant in concrete terms at the moment and in the context in which the processing is conducted via the screen of a *PC* or *smartphone*. This dynamic atomises the information, which is then recombined and given sense (and actual relevance) in the digital space and times of the *websites* and *apps* where the processing takes place; it is very clear how, especially when multiple operators are involved and the operations carried out are complex and articulate, this can ensure a greater level of detail in the information provided, and more precision and fluidity in the very process of its provision, in line with the provisions of *Recital* 58 of the GDPR, as previously mentioned in these pages.

We could say that the model in question upends the rules for administering privacy information in some way, at least the way they have been interpreted in practice since the ‘nineties. With the dynamic *ex-post* model, the information to provide to data subjects is finally freed from the imaginary state it has been acknowledged to date: that of piles of paperwork gathered round the edges of a desk, tiny print and “mandatory” signature lazily applied to the foot of the documents. Prospectively, the dynamic *ex-post* model could prove capable of clearing the encrustations of a bureaucratic dimension that should not, or should no longer belong to *privacy*.

In this respect, it is interesting to note how this approach appears to correspond to the renewed regulatory language of the GDPR, which seems to show some differences in its terminology with respect to the previous framework. For example, in Directive 95/46/CE we find an almost homogeneous use of the term “*informazioni*” (information).

On the other hand, in the domestic implementing regulations, and more recently in Legislative Decree 196/2003, the Italian legislature makes repeated use of the term “*informativa*” (information notice) (in particular, see article 13, Legislative Decree

196/2003 prior to the adjustments made by Legislative Decree 101/2018). With the GDPR, which returns to the plural of the term use for the first time in the directive, we now talk about "*informazioni*". In turn, even Legislative Decree 196/2003, as amended by Legislative Decree 101/2018, changes course and tends to use the expression "informazioni" (see, for example, articles 2-*septies*, 78, 80, 81, 82, 96, 105, 111-*bis* and many others), although in some provisions the term "*informativa*" (information notice) still appears.

This is certainly not a question of mere terminology: the more frequent use of the term "*informazioni*" opens the idea of a plural and dynamic nature that the term "*informativa*" (information notice) is unable to express, being bound to the classic bureaucratic image of reams of paper filled with small print attached to the terms and conditions of a contract.

The dynamic *ex-post* approach also appears to be based on the very recent provisions on the transparency of the information concerning *on-line* advertising contained in the *Digital Services Act*[9], the draft of the European regulation presented by the European Commission on 15 December 2020 (in particular, see articles 24 and 36; see also articles 29 and 30, for large scale *on-line* platforms). In this sense, it may be interesting to note how for *on-line* platforms that display advertising on their *on-line* interfaces, article 24 establishes the obligation to ensure that recipients of the service are able to identify the information provided by the platforms, "*for each specific advertisement displayed to each individual recipient, in a clear and unambiguous manner and in real time*".

[9] Cf. *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*. This proposal of the European Commission aims to reform the regulatory strategy of the digital market in Europe, by introducing new obligations and responsibilities for digital mediation platforms in favour of greater transparency and equity.

3. Future prospects and *Privacy Dynamic Targeting*. Algorithms as the antidote to algorithms

The dynamic *ex-post* model we describe in the previous paragraphs highlights innovative solutions and ideas that fully grasp the spirit of the provisions of article 12 (7) of the GDPR and *Recital* 58, and develop the regulatory content in an original way. These innovative solutions and ideas could easily be accompanied by others in the future.

One such idea could centre on an atypical, original use of the behavioural profiling algorithms usually used to analyse and record *web* pages visited, web searches and the preferences expressed during interactions with sites and *apps* for commercial and statistical purposes. Given that today it's not surprising to see advertising *banners* promoting products we already want (which is effectively what advertising algorithms do), this would make it easier for data subjects to disable *tracking* (which, hopefully, was previously authorised) and exercise the right to *opt-out*.

The algorithms in this sense could be the antidote to themselves.

Our proposal is to direct the potential of the use of algorithms, if developed in an intelligent way, toward different purposes with respect to those typically commercial or statistical, making the personalised profiling of data subjects more *pro-privacy* through a sort of *behavioural targeting* intended to favour greater uniformity in the experience of the various virtual spaces visited by browsers. This way, for example, if site *x* registers an objection to processing, this objection is also proposed in site *y* so as to ensure that the experience effectively and organically adheres to the *privacy* preferences expressed by the data subject. We could define this kind of initiative as *Privacy Dynamic Targeting*: *Apps* and *websites* dynamically "follow" or, better, "accompany" data subjects, analysing their behaviour and recording their preferences (also) with the purpose of uniformly ensuring their informational self-determination in each of the digital scenarios they encounter. The effect in these

cases would be that of systematically and coherently personalising the privacy-information experience to the advantage of the data subjects. Now, it could be argued that this targeting activity is unlikely to effectively distinguish the different digital contexts in which the data subject requests the exercise of his/her rights and, consequently, to "anticipate" his/her choices taking into account the peculiarities of each context: thus, for example, a user, while he/she might like a profiling for commercial purposes based on the clothing products searched online, could at the same time have reasons to object to the profiling that takes place on the basis of more sensitive information; at that point, a uniform application of the predictive algorithm could hinder the web browsing experience. However, such a criticality could be overcome in light of the consideration that Privacy Dynamic Targeting will limit itself to envisaging the exercise of the right requested on previous occasions, recommending this option without imposing it in any way.

By exploiting algorithms as an antidote to algorithms, *Privacy Dynamic Targeting* would give rise to a type of personal data processing that could well find its roots in the legitimate interest of the controller and interested third parties as per article 6 (1)(f) of the GDPR. The overriding legitimate interest with respect to the other rights and freedoms of data subjects would probably be far more convincing and justified in this case, considering that the processing would be directly instrumental, in terms of effectiveness and *accountability*, in facilitating compliance with article 12 of the GDPR on data subject rights. Although in a different context, the Italian Data Protection Authority also seems to be moving in a similar direction; on the subject of the use of *social media* by children under fourteen years of age, in a recent intervention a member of the Authority affirmed that "*Not using the technologies used to impose themselves (social media) on the global markets and attract billions of users, or not using them with the same determination to protect those who would be exposed to unsustainable risks is neither tolerable, ethically acceptable nor legally defensible*"[10]. These words appear to have a logic similar to the fundamental concepts of *Privacy Dynamic Targeting*.

[10] Cf. G. Scorza, Commissioner of the Italian Data Protection Authority, "*Now let us keep children out of social networks - Intervention by Guido Scorza*", available here https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9523881 (last acc. 2021/05/28).

4. *Legal design* and integration between privacy information and data subject request systems

We mentioned that in the "dynamic *ex-post*" model, the information is administered through *pop-up banners* or "*privacy*" keys the data subject is invited to click on. But *accountability* allows data controllers to go further and experiment with *legal design* solutions able to integrate the information functions described above with functions for acknowledging requests for the exercise of the data subject rights provided for under articles 15-22 of the GDPR.

In the direction of a more intense interactivity of the information features of the app and website, it is impossible not to mention again art. 29 of the draft Digital Services Act, which requires very large online platforms that use recommendation systems to specify "*in their terms and conditions, in a clear, accessible and easily comprehensible manner, the main parameters used in their recommender systems, as well as any options for the recipients of the service to modify or influence those main parameters that they may have made available, including at least one option which is not based on profiling, within the meaning of Article 4 (4) of Regulation (EU) 2016/679*". Although the reference to the "*terms and conditions*" suggests an approach which is still excessively static and unbalanced *ex ante*, it should nevertheless be highlighted that, in the next paragraph we read that, where several options are available to data subjects, "*very large online platforms shall provide an easily accessible functionality on their online interface allowing the recipient of the service to select and to modify at any time their preferred option for each of the recommender systems that determines the relative order of information presented to them*"[11]. In this regard, it would be appropriate to clarify, in the art. 29 of the Digital Services Act, that this functionality should include the direct provision of clear summary information and take into account the variety of contexts in which the recommendation system operates - a social network is not the same as an

[11] 'Recommender system' means, according to the first draft of Digital Services Regulation, a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service, including as a result of a search initiated by the recipient or otherwise determining the relative order or prominence of information displayed.

environment of interconnected things in a smart city - as well as consider the multiplicity of legal bases for the possible processing of personal data related to the same recommendation system (not to be limited only to users' consent, but inevitably to be extended also to legal obligations or to the legitimate interest of the controllers, in some scenarios).

In this sense, the information *banners* and privacy keys scattered about the *web* pages and the various sections of the *apps* could also be equipped with functionalities that allow data subjects to exercise rights more pertinent to the information displayed by each site. Having discharged the informational function, the *banners* and *privacy* keys would become minimised peripheral control centres able to ensure immediate delivery of requests in accordance with articles 15-22 of the GDPR and, in some cases, their acknowledgement; naturally, the possibility of sending requests through the traditional channels (for example via *e-mail*) would remain. This would add a dynamic request acknowledgement system to an already dynamic information system, guaranteeing a real and beneficial opportunity to involve data subjects in the dynamics of the processing of their personal data, inherent to every digital service but often invisible to the eye of your common or garden "internaut".

A solution of this kind could find frequent application, for example, in all cases in which the processing is based on the legitimate interest of the controller or third parties, under article 6 (1)(f) of the GDPR. In such cases, under article 21 (1) of the GDPR, data subject shall "*have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her* [whenever the processing is based, as mentioned, on point (f) of article 6(1)]*, including profiling* [...]"; for its part, the "*controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims*".

In this way, at the very moment data subjects are presented with information on a given service offered by the platform (for example, the purpose of processing and the

underlying legitimate interest), this could include information on the possibility of exercising their right to object with immediate effect. Indeed, in many cases the controller's assessment of the possibility of meeting the data subject's objection may be carried out *ex-ante*, in a systematic, generalised way; naturally on the sole condition that the assessment gives a positive result for the data subject and not the other way round. In a dynamic model, all it would take would be one *click* and the data controller would no longer be able to carry out the processing.

Again, when presented with information in the context of a specific section of an *app*, *privacy* buttons could be provided for contesting the accuracy and requesting correction to the data, as per article 16 of the GDPR, as well as *pop-ups* that could give data subjects the possibility to restrict the processing, as per article 18 (1)(a) of the GDPR, to "*for a period enabling the controller to verify the accuracy of the personal data*".

In any event, here we are not referring to those intrusive *banners* strategically designed to block the view of the *web* pages, like the ones associated with *cookies*, but rather to entirely optional buttons and keys, certainly not designed to disturb the browsing experience but enrich it, making it possible to exercise the rights provided for under articles 15-22 of the GDPR with immediacy and somehow "empowering" the data subjects themselves.

5. Closing remarks

In conclusion, while the static *ex-ante* model, like the one developed by Apple, is still anchored to traditional information administration criteria (even if in innovative and creative ways) and risks collateral effects on the free economic initiative and freedom of expression of developers, the dynamic *ex-post* model adopted by other operators seems to offer a clearer idea of the future of *privacy*.

By abandoning the concept of the privacy information notice as a singular, static summary of information on the processing of personal data (as we find in *nutrition labels*, or, continuing the metaphor, in a static *menu* abstractly describing ingredients and dishes), the dynamic *ex-post* model disaggregates the information and releases it precisely in the digital spaces where the processing effectively takes place (as would be the case, continuing the nutritional metaphor, of a waiter describing the qualities and characteristics of the dishes as they're being served, in real time). In the future, the dynamic *ex-post* model could evolve further and develop in at least two directions. One could involve the use of algorithms not already serving typically commercial or statistical purposes, for profiling data subjects according to the *privacy* preferences expressed in the various digital spaces they visit, thereby ensuring uniformity in their digital self-determination. This corresponds to the *Privacy Dynamic Targeting* we mentioned earlier. The other could involve combining the information functions with the functions for the exercise of the rights provided for under articles 15-22 of the GDPR, which could finally turn the concept of *privacy* into something live and interactive.

The path is set: to give renewed sense to the obligations established under articles 12, 13 and 14 of the GDPR we have to try innovative solutions and revolutionise the traditional schemes for administering privacy information. Above all, we have to free ourselves of our current formalistic and abstract concept of digital *privacy*, courageously and profoundly change its image and convince ourselves of its authentic popular nature, as much as the popular nature of a commercial or advert.