Feedback to the Guidelines on the use of cookies and other tracking tools of the Italian Data Protection Authority

Nataliia Bielova, Cristiana Santos

Italian Data Protection Authority - Garante per la protezione dei dati personali

RE: ***Consultazione sulle "Linee guida sull'utilizzo di cookie e di altri strumenti di tracciamento"***

Dr. Nataliia BIELOVA
Inria, France
nataliia.bielova@inria.fr

Dr. Cristiana SANTOS
University of Utrecht, The Netherlands
c.teixeirasantos@uu.nl

We would like to submit for the *Garante*'s consideration the comments below. We use this occasion to share **our research on legal and technical analysis of EU requirements for cookies and cookie banners**, that also contains techniques to verify compliance at scale[1].

Each comment precedes by a quotation from the proposed text by the *Garante* followed by our translation to English highlighted in grey color.

3. Altri strumenti di tracciamento

- We would like to draw Authority's attention on the distinction between *cookies, fingerprinting* and other tracking technologies, profiling and identification (direct or indirect) of users:

"Il medesimo risultato può essere conseguito anche mediante l'utilizzo di altri strumenti (c.d. "identificativi attivi" e "passivi", questi ultimi presupponendo la mera osservazione), che consentono di effettuare trattamenti analoghi a quelli sopra indicati."

"The same result can also be achieved through the use of other tools (so-called" active "and" passive "identifiers, the latter assuming mere observation), which allow for processing similar to those indicated above."

- The Authority proposes to distinguish "active" (*cookies* and other stateful identifiers) and "passive" (*fingerprinting* and similar technologies) and reason about them independently from the discussion on non-personal data collection, such as preferences on languages or device types;

"Le informazioni codificate nei cookie possono includere dati personali, come un indirizzo IP, un nome utente, un identificativo univoco o un indirizzo e-mail, ma possono anche contenere dati non personali, come le impostazioni della lingua o informazioni sul tipo di dispositivo che una persona sta utilizzando per navigare nel sito."

[1] Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. Cristiana Santos, Nataliia Bielova and Célestin Matte.*International Journal on Technology and Regulation, 2020.*

"The information encoded in cookies may include personal data, such as an IP address, username, unique identifier or email address, but may also contain non-personal data, such as language settings or information about the type of device that a person is using to browse the site."

- However, from a technical perspective, the distinction between the active/passive data collection and personal/non-personal data stored in a cookie (or collected by other means) is not meaningful. The first question that instead needs to be answered is: "**Is the data collected enough to recognise[2] the end-user in a given group?**" Cookies may contain enough information for it (when an identifier is stored in a cookie) or not (when a language preference is stored), and this very same reasoning applies to fingerprinting: it may be enough information (e.g., based on passive, but also active Canvas fingerprinting) or not (when only UserAgent is stored).
- The second question is "**How is the data used?** and **Is it combined with other sources?"** Data that is not enough to recognise a user (e.g., her language preference stored in a cookie or UserAgent collected from a fingerprint) can be collected with other data that makes a user identifiable. In our recent work, we showed how unique (and hence recognizable) users are based on their browser extensions: even though one extension is not enough, a combination of all extensions makes a user highly identifiable.[3]
- Finally, following the cognition of the EDPB, only the **purpose of each tracking technology**[4] has legal effects on using that technology (independently whether it is a cookie, fingerprinting or any other form of tracking technique or profiling), and therefore, only purposes can determine the need for consent or the exemption therefrom, and can be used to verify compliance.

"Sussiste tuttavia una non trascurabile differenza, sulla quale l'Autorità intende porre l'accento, tra l'impiego di una tecnica attiva quale quella relativa ai cookie ed una passiva, come quella relativa al fingerprinting.

Nel primo caso, infatti, l'utente che non intenda essere profilato, oltre ovviamente a poter rifiutare il proprio consenso, o a ricorrere alle tutele di carattere giuridico connesse all'esercizio dei diritti di cui al Regolamento, ha anche la possibilità pratica di rimuovere direttamente i cookie, in quanto archiviati all'interno del proprio dispositivo."

"There is, however, a significant difference, on which the Authority intends to emphasize, between the use of an active technique such as that relating to cookies and a passive one, such as that relating to fingerprinting.

---

[2] We use the word "recognize" to mean "identifiable" (GDPR Recital 26) to underline the fact that the person does not need to be identified, that is it is enough to have information to recognize the user based on her characteristics.

[3] To Extend or not to Extend: on the Uniqueness of Browser Extensions and Web Logins. Gábor György Gulyás, Dolière Francis Somé, Nataliia Bielova and Claude Castelluccia. *Workshop on Privacy in the Electronic Society (WPES 2018) at ACM CCS 2018.*

[4] Article 29 Working Party, "Opinion 03/2013 on Purpose Limitation (WP203).

In the first case, in fact, the user who does not intend to be profiled, besides obviously being able to refuse his consent, or to resort to the legal protections related to the exercise of the rights referred to in the Regulation, also has the practical possibility of directly removing cookies, as they are stored on your device."

- We do not agree with this observation with regard to the deletion of cookies. Unfortunately, not all cookies can be easily deleted because (1) the same third party content is often used to deliver website functionality and advertising cookies; (2) some cookies get re-created (respawned) even after their deletion; (3) other browser storages (HTML5 localStorage, cache, etc) are not easy to clean for regular users because not all browsers provide such settings. Also, first-party cookies are often used in a third-party context, thus third-party cookie blocking is rendered ineffective against those.
- Finally, even if cookies are effectively deleted by the user, in practice, **the action of cookie deletion does not have legal effects** on the parties that installed such cookies, since it's not recognized as an expression of refusal of consent. Therefore, information collected on the server can still be processed (including RTB) even though the user has deleted the cookie.

"Diversamente, con riguardo al fingerprinting, l'utente non dispone di strumenti autonomamente azionabili, dovendo necessariamente far ricorso all'azione del titolare. Ciò in quanto quest'ultimo fa uso di una tecnica di accesso che non presuppone l'archiviazione di informazioni all'interno del dispositivo dell'utente, bensì la mera lettura delle configurazioni che lo contraddistinguono rendendolo identificabile, ed il cui esito si sostanzia in un "profilo" che resta nella sola disponibilità del titolare, cui l'interessato non ha, ovviamente, alcun accesso libero e diretto."

"Otherwise, with regard to fingerprinting, the user does not have autonomously operable tools, necessarily having to resort to the action of the owner. This is because the latter makes use of an access technique that does not presuppose the storage of information inside the user's device, but the mere reading of the configurations that distinguish it, making it identifiable, and the outcome of which is substantiated in a "Profile" that remains solely available to the owner, to which the data subject obviously has no free and direct access."

- While it's true that there is no 100% effective protection from fingerprinting, some browsers integrate a form of diversification and thus render fingerprinting less useful. However, **protecting from fingerprinting has no legal effects on compliance**.
- The only characteristics that matter in the usage of fingerprinting is **its purpose** and whether such **purpose requires consent.** Fingerprinting is often used for security (patching vulnerable systems, bot and fraud prevention, augmented authentication - see pages 23-24 or our recent survey on browser fingerprinting)[5] that does not seem to require consent.

[5] Browser Fingerprinting: A survey. Pierre Laperdrix, Nataliia Bielova, Benoit Baudry and Gildas Avoine. *ACM Transactions on the Web (ACM TWEB), 2020.*

4. La classificazione di cookie ed altri strumenti di tracciamento

"I cookie e, in buona misura, gli altri strumenti di tracciamento, possono avere caratteristiche diverse sotto il profilo temporale e dunque essere considerati in base alla loro durata (di sessione o permanenti), ovvero dal punto di vista soggettivo (a seconda che il publisher agisca autonomamente o per conto della "terza parte")."

"Cookies and, to a large extent, other tracking tools, may have different characteristics in terms of time and therefore be considered based on their duration (session or permanent), or from a subjective point of view (depending on whether the publisher act independently or on behalf of the "third party")."

- From a technical point of view, we don't agree that these distinctive characteristics (duration and subject) make any difference:
    - Duration: we have seen in our recent works that the expiration date of permanent cookies is often updated and thus is not reliable, while session cookies can get re-created even after their elimination by the user;
    - First or third-party: third parties today have numerous techniques to "hide" behind the first-party domain name, including recently found techniques such as CNAME cloaking.[6]

"Analogamente, gli altri strumenti di tracciamento possono essere catalogati secondo una serie di criteri diversi, dei quali il principale resta, tuttavia, la finalità con la quale vengono utilizzati: tecnica o di natura commerciale."

"Similarly, the other tracking tools can be cataloged according to a series of different criteria, of which the main one remains, however, the purpose for which they are used: technical or commercial."

- We underline that what defines the use of cookies and tracking technologies is **only their purpose** and not its technical characteristics - this opinion has also been often mentioned in the recent French DPA Guidance.[7]
- Moreover, we emphasize that all tracking technologies, either cookies, other storages or browser fingerprinting, undergo the same requirement that **only their purpose determines** whether these require consent or not.

---

[6] https://medium.com/nextdns/cname-cloaking-the-dangerous-disguise-of-third-party-trackers-195205dc522a

[7] CNIL Guidelines on the use of cookies and other trackers, 2020, available online at https://www.cnil.fr/sites/default/files/atoms/files/lignes_directrices_de_la_cnil_sur_les_cookies_et_autres_traceurs.pdf

"E tuttavia la classificazione che risponde alla ratio della disciplina di legge e dunque anche alle esigenze di tutela della persona, è quella che si basa, in definitiva, su due macro categorie:
- i cookie tecnici [...]
- i cookie di profilazione [...]"

"And yet the classification that responds to the rationale of the law and therefore also to the protection needs of the person, is that which is ultimately based on two macro categories:
- technical cookies [...]
- profiling cookies [...]"

- While analysing the purposes for cookies[8] and lawfulness of purposes within the IAB Europe TCF[9], we found out that many of the declared purposes are hard to map into only one of the two categories (hence, being multipurposes). For example,
    - some companies provide a technical description of cookies instead of purposes that can help identify whether consent is needed (e.g., "Session Pixel Tracker"),
    - in IAB Europe TCF a purpose such as "Technically deliver ads and content" seem to mix technical necessity and advertising.

5. Normativa applicabile

"Per l'impiego di cookie tecnici, in virtù della funzione assolta e nei limiti ed alle condizioni richiamate, il titolare del trattamento sarà assoggettato al solo obbligo di fornire l'informativa, anche eventualmente inserita all'interno dell'informativa di carattere generale, rientrando il loro impiego in una ipotesi codificata di esenzione dall'obbligo di acquisizione del consenso dell'interessato;"

"For the use of technical cookies, by virtue of the function performed and within the limits and conditions recalled, the data controller will be subject to the sole obligation to provide the information, also possibly included in the general information, re-entering their use in a codified hypothesis of exemption from the obligation to acquire consent of the interested party"

- We believe that **information on the purpose and legal basis should be given for all cookies and tracking technologies**, including 'technical cookies" (and not only indicated that technical cookies are used).
- Some DPAs advocate that all cookies should – as a best practice – declare their purpose. The UK, Greek, Finnish and Belgian DPAs[10] endorse as a good practice

[8] On Compliance of Cookie Purposes with the Purpose Specification Principle. Imane Fouad, Cristiana Santos, Feras Al Kassar, Nataliia Bielova and Stefano Calzavara. *International Workshop on Privacy Engineering (IWPE 2020).*
[9] Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers? Célestin Matte, Cristiana Santos, Nataliia Bielova. *Annual Privacy Forum (APF 2020).*
[10] UK DPA, "Guidance on the rules on use of cookies and similar technologies", 2020; Finnish DPA, "Guidelines on confidential communications", 2020; Greek DPA, "Guidelines on cookies and trackers", 2020; Belgium DPA, "Guidance on cookies and other tracking technologies", 2020.

the disclosure of clear information about the purposes of cookies, including strictly necessary ones. The guidance of the 29WP (WP188)[11] notes that although some cookies may be exempted from consent, they are part of a data processing operation, therefore publishers still have to comply with the obligation to inform users about the usage of cookies prior to their setting.

- Unfortunately, in practice, only around 5% of HTTP cookies[12] (not including other tracking technologies) have well-defined and explicit purposes presented in a table, yet few of these 5% are not specific enough to establish whether consent is needed.

6.1 Il c.d. "*scrolling*" e il divieto di *cookie wall*

Scrolling

"Lo scrolling, tuttavia, può essere una componente di un più articolato processo che consenta comunque all'utente di segnalare al titolare del sito, con la generazione di un preciso pattern, una scelta inequivoca nel senso di prestare il proprio consenso all'uso dei cookie.
In questo senso, già nelle FAQ in materia di informativa e consenso per l'uso dei cookie del 3 dicembre 2014 si è affermato che qualora le soluzioni adottate "siano in grado di generare un evento, registrabile e documentabile presso il server del gestore del sito (prima parte), che possa essere qualificato come azione positiva dell'utente", idonea a manifestare in maniera inequivoca la volontà di prestare un consenso al trattamento, esse saranno da ritenersi "in linea con i requisiti di legge"."

"Scrolling, however, can be a component of a more complex process that still allows the user to report to the owner of the site, with the generation of a precise pattern, an unequivocal choice in the sense of giving their consent to the use of cookies.
In this sense, already in the FAQ on information and consent for the use of cookies of 3 December 2014 it was stated that if the solutions adopted "are able to generate an event, which can be recorded and documented on the site manager's server (first part), which can be qualified as a positive action of the user ", suitable to express unequivocally the will to give consent to the treatment, they will be considered" in line with the legal requirements "."

- Whether using solutions that "*are able to generate an event, recordable and documentable at the site manager's server (first part), which can be qualified as a positive action of the user", suitable to unequivocally manifest the will to lend a consent to the processing*", or whether using "*mouse movements within the site (...) able to report more easily, compared to traditional virtual buttons, positive and unambiguous user actions as a form of registration of the consent expressed by the user for the*

[11] Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising, adopted December, 2011.
[12] On Compliance of Cookie Purposes with the Purpose Specification Principle. Imane Fouad, Cristiana Santos, Feras Al Kassar, Nataliia Bielova and Stefano Calzavara. *International Workshop on Privacy Engineering (IWPE 2020).*

installation of cookies" — what is legally recognized is the **user's active behavior**. Planet49 Judgment (in paragraph 54) made even more precise this requirement. This ruling asserts that **"only active behavior on the part of the data subject with a view to giving his consent may fulfil that requirement" and this** wording ('with a view to') denotes the element of volition and willfulness towards giving an affirmative consent. An active behavior leaves **no scope for interpretation** of the user's choice, which must be distinguishable from other actions (even if recordable and documentable, such as the options the Garante suggests). As such, behaviors presenting a margin of doubt — such as scrolling — do not deliver a choice and therefore are void (29WP187).[13]

- According to the CNIL[14], silence (for example, the absence of clicking on a button, or even scrolling, as depicting lack of action from the user's side) can be considered valid refusal (Article 2, paragraph 30: "*if the consent must result in a positive action by the user, the user's refusal can be inferred from his silence. The expression of the user's refusal must therefore not require any action on his part*" (our translation).

Cookie walls

"*Tale meccanismo, non consentendo di qualificare l'eventuale consenso così ottenuto come conforme alle caratteristiche imposte dal Regolamento, e segnatamente al suo art. 4, punto 11, è da ritenersi illecito, salva l'ipotesi -da verificare caso per caso- nella quale il titolare del sito offra all'interessato la possibilità di accedere ad un contenuto o a un servizio equivalenti senza prestare il proprio consenso all'installazione e all'uso di cookie.*

"This mechanism, not allowing to qualify any consent thus obtained as complying with the characteristics imposed by the Regulation, and in particular with its art. 4, point 11, is to be considered illegal, except for the hypothesis - to be verified case by case - in which the owner of the site offers the interested party the possibility of accessing an equivalent content or service without giving his consent to the installation and the use of cookies."

- The criteria of equivalence of content or service should be evaluated both qualitative and quantitatively. We are alerting to the fact that the use of "equivalent content or service" should not be detrimental to the user, which could render a not freely given consent. This means facing significant negative consequences (Recital 42 of the GDPR), which could consist in different situations, suchlike when a service is downgraded (EDPB Guidelines 05/2020)[15], which could substantiate a reduced service, or accessing the full service would require paid services or extra costs.

[13] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent' (WP187, 13 July 2011).
[14] CNIL Guidelines on the use of cookies and other trackers, 2020, available online at https://www.cnil.fr/sites/default/files/atoms/files/lignes_directrices_de_la_cnil_sur_les_cookies_et_autres_traceurs.pdf
[15] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, 2020.

- In our recent research[16], we analysed the practice of *cookie walls* together with legal, technical and design researchers and conclude that "*this design choice increases the tension between interactive separation of user activities and the requirement to allow the user to freely give their consent. In addition to this primary design and legal tension, the lack of an ability to reject consent—alongside the inability to use the web resource without making this forced choice—represents an additional barrier to the user's ability to make a specific and informed decision.*"

6.2 La reiterazione nella richiesta di consenso

"Il consenso, una volta correttamente acquisito, non dovrà essere nuovamente richiesto se non all'eventuale mutare di una o più delle condizioni alle quali è stato raccolto ovvero quando sia impossibile, per il gestore del sito web, avere contezza del fatto che un cookie sia stato già in precedenza memorizzato sul dispositivo per essere nuovamente trasmesso, in occasione di una successiva visita del medesimo utente, al sito che lo ha generato;"

"Once correctly acquired, consent must not be requested again except for the possible change of one or more of the conditions under which it was collected or when it is impossible for the website manager to be aware of the fact that a cookie is previously stored on the device to be transmitted again, on the occasion of a subsequent visit by the same user, to the site that generated it";

- We agree with this positioning regarding the correct consent registration of the user's choice. We recommend the usage of cryptographic primitives to ensure that the choice of the user has never been forged —see our feedback to the public consultation of the CNIL on the guidance for cookies and other trackers.[17]
- Moreover, the choice of the user in the consent interface must correspond to the technical user's choice stored in the system. Using the open source Cookie Glasses tool,[18] it is possible to verify whether consent registers the user's choice given in the user interface for consent banners that implement IAB Europe Transparency and Consent Framework v1.1, however this task is more complex for other types of banners.

7. Privacy by design and by default in relation to cookies and other tracking tools

7.1 The mechanism for acquiring consent

[16] Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. C. Gray, C. Santos, N. Bielova, M. Toth, D. Clifford. Accepted for publication at ACM CHI 2021.
[17] M. Toth, N. Bielova, C. Santos, V. Roca, and C. Matte. Contribution to the public consulta- tion on the CNIL's draft recommendation on "cookies and other trackers", 2020. Research report, https://hal.inria.fr/hal-02490531
[18] Browser extension tool for IAB Europe TCF v1.1 is available at https://github.com/Perdu/Cookie-Glasses

"Tuttavia, poiché occorre assicurare anche la libertà di scelta di chi invece intenda accettare di essere profilato, il Garante suggerisce che i gestori dei siti web implementino un meccanismo in base al quale l'utente, accedendo alla home page (o ad altra pagina) del sito web, visualizzi immediatamente un'area di dimensioni sufficienti da costituire una percettibile discontinuità nella fruizione dei contenuti della pagina web che sta visitando, che sia parte integrante di un meccanismo che, pur non impedendo il mantenimento delle impostazioni di default, permetta anche l'eventuale espressione di una azione positiva nella quale deve sostanziarsi la manifestazione del consenso dell'interessato."

"However, since it is also necessary to ensure the freedom of choice of those who intend to accept being profiled, the Guarantor suggests that the website operators implement a mechanism whereby the user, by accessing the home page (or other page) of the website, immediately displays an area of sufficient size to constitute a perceptible discontinuity in the use of the contents of the web page you are visiting, which is an integral part of a mechanism which, while not preventing the maintenance of the default settings, also allows the possible expression of a positive action in which the manifestation of the consent of the interested party must be substantiated."

- The mechanism described seems to resonate with the use of a *consent wall*. A consent wall is a design choice that blocks access to the website until the user expresses her choice regarding tracking. This design choice allows a user to select between acceptance and refusal; however, the concrete use of the website is blocked until a choice has been made. Differently from "*cookie wall"*, this practice allows the user to make a choice between acceptance and refusal. A consent wall appears to be unnecessarily disruptive to the use of a website.
- In this regard, a cautionary approach needs to be accounted for. Recital 32 of the GDPR states that the consent request should not be unnecessarily disruptive to the use of the service for which it is provided. In our own opinion of this Recital, expressed in our recent publication[19], consent wall implements an unnecessary disruption to the use of a website, while the website should still be accessible even if the user didn't respond to the consent request. If there are other ways to show the banner without blocking (disturbing) the access to the service, or disrupting the user experience, then it is preferred to a consent wall.
- Thus, we argue that **consent walls do not configure a valid design for consent mechanisms**; they are confusing and unnecessarily disruptive of the user experience. Other consent design implementations could be sought while engaging the users. *We argue that the mere appearance of a consent wall presses the user to decide, which collides with the requirement of a freely given consent (Arts. 4(11) and 7(4).*

"Qualora l'utente scegliesse, com'è nella sua piena disponibilità, di mantenere quelle impostazioni di default e dunque di non prestare il proprio consenso al posizionamento dei cookie o all'impiego di altre tecniche di profilazione, dovrebbe dunque limitarsi a chiudere tale

[19] Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. Cristiana Santos, Nataliia Bielova and Célestin Matte.*International Journal on Technology and Regulation, 2020.*

finestra o area mediante selezione dell'apposito comando usualmente utilizzato a tale scopo, cioè quello contraddistinto da una X di regola posizionata in alto a destra del banner medesimo, senza essere costretto ad accedere ad altre aree o pagine a ciò appositamente dedicate. Si garantirebbe, in tal modo, che appunto by default, l'interessato che non intenda esprimere il proprio consenso non sia in alcun modo tracciato o profilato".

"If the user chooses, as it is in his full availability, to keep those default settings and therefore not to give his consent to the placement of cookies or to the use of other profiling techniques, he should therefore limit himself to closing this window or area by selecting the appropriate command usually used for this purpose, ie the one marked by an X usually positioned at the top right of the banner itself, without being forced to access other areas or pages specifically dedicated to this. In this way, it would be ensured that precisely by default, the interested party who does not intend to express his consent is not in any way tracked or profiled".

- The Authority refers to the expression of refusal to consent through the action of closing the banner (which results from other than the typical action of clicking on the reject button).
- We note that while website operators are free to use or develop consent flows that suit their organization, we believe that **the standardization of design elements should be taken in consideration**, in particular to the options for accept/reject tracking, pursuant to transparency, usability and clarity.
- Accordingly, we suggest that refusal could also be made in an unambiguous way by clicking on the reject button, which seems to be more akin to the legitimate expectations of the end-user.
- We also assert the action of closing a banner might consist in an unambiguous act if not duly explained what it is meant for in a clear and understandable way in that banner.

"A tale riguardo, il Garante sottolinea tuttavia l'importanza di avviare nelle sedi più opportune e tra tutti i soggetti interessati (accademia, industria, associazioni di categoria, decisori, stakeholder etc.) una riflessione circa la necessità dell'adozione di una codifica standardizzata relativa alla tipologia dei comandi, dei colori e delle funzioni da implementare all'interno dei siti web per conseguire la più ampia uniformità, a tutto vantaggio della trasparenza, della chiarezza e dunque anche della migliore conformità alle regole".

"In this regard, however, the Guarantor underlines the importance of initiating a reflection on the need to adopt a standardized codification in the most appropriate fora and among all interested parties (academia, industry, trade associations, decision makers, stakeholders etc.) relating to the type of commands, colors and functions to be implemented within the websites to achieve the widest uniformity, to the benefit of transparency, clarity and therefore also better compliance with the rules ".

- We welcome this position and we emphasize the need for neutral and standardized design patterns to be more explicitly defined by the DPAs as best practices.[20] Choice

[20] Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. C. Gray, C. Santos, N. Bielova, M. Toth, D. Clifford. Accepted for publication at ACM CHI, 2021.

and design of configurations has been proven to strongly impact the end-user decision-making towards acceptance through the use of manipulative design choices (also known as “dark patterns”).[21]-[22] Design choices related to an unbalanced choice in a consent banner can consist, for example, of “False Hierarchy” and “Aesthetic manipulation”[23], both at the first and second layers of the banner.

“Sempre all’interno di questa stessa area dovrebbero trovare collocazione anche due ulteriori comandi idonei a garantire il cd. “diritto di ripensamento” e di revoca del consenso agli utenti che, avendo già effettuato una specifica scelta al momento del primo accesso al sito web, intendano successivamente optare per una scelta diversa. A tali utenti, proprio in ragione della scelta già compiuta e debitamente registrata, ad ogni accesso successivo al primo non verrà infatti riproposto il meccanismo del banner, ma la pagina iniziale del sito dovrà comunque rendere sempre disponibile il link alla privacy policy nonché all’area dedicata alle scelte di maggiore dettaglio.”

“Also within this same area there should also be two additional commands suitable for guaranteeing the cd. "Right to reconsider" and to withdraw consent to users who, having already made a specific choice at the time of the first access to the website, they intend to subsequently opt for a different choice. To such users, precisely because of the choice already completed and duly registered, the banner mechanism will not be re-proposed at each subsequent access to the first, but the home page of the site must always make available the link to the privacy policy as well as to the area dedicated to more detailed choices.”

- The Garante is proposing a new right -- the “right to reconsider”, additional to the GDPR right to withdrawal, to assure the user the possibility to subsequently opt for a different choice. We wonder if such an additional right is consistent with practices of other EU member-states.
- In this line, we propose to clarify such statements to avoid confusion between the afforded GDPR rights. Instead, we note that the use of an explicit mechanism called “*configure my privacy options*” (or an intuitive name alike) could be used to manage the preferences of the user at any given time. Such mechanism could assume the shape of a standardized icon placed in an accessible way to the user (e.g. located at the bottom left of the screen)[24].

[21] Utz, Christine, Martin Degeling, Sascha Fahl, Florian Schaub and Thorsten Holz. “(Un)informed Consent: Studying GDPR Consent Notices in the Field.” *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019

[22]CNIL’s 6th Innovation and Foresight Report ‘Shaping Choices in the Digital World, ‘From dark patterns to data protection: the influence of UX/UI design on user empowerment’, 2019, https://linc.cnil.fr/fr/ip-report-shaping-choices-digital-world.

[23] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs, ‘The Dark (Patterns) Side of UX Design’ (Proceedings of the CHI Conference on Human Factors in Computing Systems ACM, New York, USA), 2018.

[24] The same reasoning is held by the CNIL in points 43-45 if its Guidelines on the use of cookies and other trackers, 2020, available online at https://www.cnil.fr/sites/default/files/atoms/files/lignes_directrices_de_la_cnil_sur_les_cookies_et_autres_traceurs.pdf

- In our recent research, we have already identified a specific requirement for consent banners called “R21 Possible to change in the future” that describes such possibility to configure privacy options in the future. An example of a best practice to follow is presented by the website *faktor.io* website in a shape of a fingerprint.[25]

“Appunto in questa area, che qui si descrive, è opportuno vengano collocati, oltre ai comandi relativi alle scelte granulari, due ulteriori comandi che consentano di modificare anche in blocco una scelta precedente; uno per acconsentire all’impiego di tutti i cookie o di altri strumenti di tracciamento per chi non vi avesse acconsentito in precedenza, l’altro per revocare, anche in unica soluzione, il consenso eventualmente già espresso. Anche tale scelta dell’utente dovrà naturalmente essere adeguatamente documentata dal titolare”

“Precisely in this area, which is described here, it is advisable to place, in addition to the commands relating to the granular choices, two further commands that allow you to modify a previous choice even in bulk; one to consent to the use of all cookies or other tracking tools for those who have not previously consented, the other to revoke, even in a single solution, any consent already expressed. This choice of the user must of course also be adequately documented by the owner”

- We agree with the inclusion of these two commands to enable global choices (accept and reject) in bulk to a set of purposes. We observe that a request for consent “per purpose” does not signify a request “per cookie”, “per publisher”, nor “per third-party”. This is also the positioning of the CNIL (paragraphs 26-28 of its Guidelines for cookies and other trackers).[26]
- We claim that the consent request for each cookie/tracker is not user-friendly and it might be too overwhelming for users -- due to usability concerns and user’s expectations and reactions to such consent dialog. We provide further details on **the argument to choose per purpose** in section 5.3.1 of our paper.[27]

“Per assicurare che gli utenti non siano influenzati da scelte di design che inducano a preferire una opzione anziché l’altra, si sottolinea l’esigenza dell’utilizzo di comandi e di

[25] Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. Cristiana Santos, Nataliia Bielova and Célestin Matte.*International Journal on Technology and Regulation, 2020.*
[26] CNIL Guidelines on the use of cookies and other trackers, 2020, available online at https://www.cnil.fr/sites/default/files/atoms/files/lignes_directrices_de_la_cnil_sur_les_cookies_et_autres_traceurs.pdf
[27] Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. Cristiana Santos, Nataliia Bielova and Célestin Matte.*International Journal on Technology and Regulation, 2020.*

caratteri di uguali dimensioni, enfasi e colori, che siano ugualmente facili da visionare e utilizzare."

"To ensure that users are not influenced by design choices that lead them to prefer one option over the other, the need to use commands and fonts of equal size, emphasis and colors, which are equally easy to view, is emphasized and use"

- With respect to user consent, we suggest even a deeper analysis of design patterns that have a direct impact on the user choice.[28]

"Per realizzare la memorizzazione delle azioni e delle scelte, anche di dettaglio, rimesse all'interessato (espressione, anche granulare, del consenso ovvero revoca del consenso precedentemente espresso mediante ripristino delle impostazioni di default), il gestore del sito web potrebbe avvalersi o di appositi cookie tecnici (in tal senso, si veda anche il considerando 25 della direttiva 2002/58/CE), oppure di altri strumenti di tracciamento diversi dai cookie o anche di ulteriori modalità la cui individuazione rientra nell'autonomia imprenditoriale del titolare, adattando opportunamente la propria condotta in modo da tenere comunque costantemente aggiornata la documentazione delle scelte compiute dall'interessato."

*"To realize the memorization of actions and choices, even in detail, remittances to the interested party (expression, even granular, of consent or withdrawal of consent previously expressed by restoring the default settings), the site manager web could make use of specific technical cookies (in this sense, see also recital 25 of Directive 2002/58 / EC), or other tracking tools other than cookies or even **additional methods whose identification falls within the entrepreneurial autonomy of the owner**, appropriately adapting their conduct in order to keep constantly updated the documentation of the choices made by the interested party"*

- We believe that the Authority refers to the use of actors that are responsible for collection and storage of consent, named "Consent Management Platforms" (CMP) in the IAB Europe TCF framework.
- We alert that it should be made clear and transparent to the end-user which role such actors would have (controller, processor and joint controller with the publisher). We raise these questions and elaborate observations in our recent feedback to the public consultation of the EDPB.[29]

7.2 I *cookie analytics* di *prima parte* e delle cd. *terze parti*

7.2 First-party analytics cookies and cd. third parts

[28] Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. C. Gray, C. Santos, N. Bielova, M. Toth, D. Clifford. Accepted for publication at ACM CHI 2021.
[29] In the "Call for Feedback regarding Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 2020" we discuss the roles of the CLP within the IAB TCF, http://www-sop.inria.fr/members/Nataliia.Bielova/opinions/EDPB-contribution-controllers-processors.pdf.

“I cookie possono anche essere utilizzati, tra l’altro, per valutare l’efficacia di un servizio della società dell’informazione fornito da un publisher, per la progettazione di un sito web o per contribuire a misurarne il “traffico”, cioè il numero di visitatori anche eventualmente ripartiti per area geografica, fascia oraria della connessione o altre caratteristiche.”

*“Cookies can also be used, among other things, to evaluate the effectiveness of an information society service provided by a **publisher**, for the design of a website or to help measure its "traffic", ie the number of visitors also possibly broken down by geographical area, time slot of the connection or other characteristics.”*

- We draw your attention to a prudent use of the qualification of “publisher” because it actually depends on how technically one evaluates the ownership of a given cookie.
- Third party cookies can be carefully hidden behind the publisher’s domain, either via CNAME cloaking mentioned above, or via third party scripts that set such cookies.
- “First-party” analytics cookies are also often synchronised with third-party cookies and hence allow for a more fine-grained tracking and merging of user’s information. We have detected a number of such synchronisation actions in our recent research.[30] This practice has also been revealed by the CNIL in their recent sanction against Carrefour France when Google Analytics cookies were integrated with Google Ads.[31]

“In questa prospettiva, il Garante reputa che, nel caso di specie, tale obiettivo debba essere conseguito attraverso il ricorso a misure di minimizzazione del dato che riducano significativamente il potere identificativo dei cookie analytics, qualora il loro utilizzo avvenga ad opera di “terze parti”.”

“In this perspective, the Guarantor believes that, in the present case, this objective must be achieved through the use of data minimization measures that significantly reduce the identifying power of analytics cookies, if their use is made by "third parties" .

- We believe that usage of analytic cookies by third-parties raises too many risks for a possible identification of the end-user and it gives such third-parties a capability to track users across websites, either with the use of cookie synchronisation or re-creation techniques that are well known today.
- We suggest the Garante to include a stronger statement, potentially similar to the one of the CNIL, stating that “*These trackers **must not in particular allow the overall***

[30] See section 4.2.3 of Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels. Imane Fouad, Nataliia Bielova, Arnaud Legout, Natasa Sarafijanovic-Djukic. *Privacy Enhancing Technologies (PoPETS 2020)*

[31] See 176 of Délibération de la formation restreinte n° SAN-2020-008 du 18 novembre 2020 concernant la société CARREFOUR FRANCE https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042563756

monitoring of the navigation *of the person using different applications or browsing different websites."* [our translation][32]

- Additionally, publishers that include any form of analytics cookies must clearly state which technology they use and for which purpose in the information page.
- Finally, we recommend not to use the term "analytics cookies" but instead "analytics purpose" because other technologies than cookies can be used for analytics in the near future.

"[...] Di regola questo effetto si ottiene integrando la struttura dell'indirizzo IP all'interno del cookie e mascherando opportune porzioni di quell'indirizzo.
Tenuto conto della rappresentazione degli indirizzi IP versione 4 (IPv4) che, costituiti da numeri interi rappresentati con 32 bit, sono usualmente rappresentati e utilizzati come sequenza di quattro numeri decimali compresi tra 0 e 255 separati da un punto, una delle misure implementabili al fine di beneficiare dell'esenzione consiste nel mascheramento almeno della quarta componente dell'indirizzo, opzione che introduce una incertezza nell'attribuzione del cookie ad uno specifico interessato pari a 1/256 (circa 0,4%).
Analoghe procedure dovrebbero essere adottate in riferimento agli indirizzi IP versione 6 (IPv6), che hanno una differente struttura e uno spazio di indirizzamento enormemente superiore (essendo costituiti da numeri binari rappresentati con 128 bit)."

"[...] As a rule, this effect is obtained by integrating the structure of the IP address within the cookie and masking appropriate portions of that address.
Taking into account the representation of IP version 4 (IPv4) addresses which, consisting of integers represented with 32 bits, are usually represented and used as a sequence of four decimal numbers between 0 and 255 separated by a period, one of the measures that can be implemented in order to to benefit from the exemption consists in masking at least the fourth component of the address, an option that introduces an uncertainty in the attribution of the cookie to a specific interested party equal to 1/256 (approximately 0.4%).
Similar procedures should be adopted with reference to IP version 6 (IPv6) addresses, which have a different structure and an enormously larger address space (being made up of binary numbers represented with 128 bits)."

- We observe that the Garante discusses here one way to generate identifiers from IP addresses.
- We draw the attention that IP addresses are often stable over time and hence, even if a user deletes her cookies, IP addresses don't change and then it's not possible to

[32] See point 51 of CNIL Guidelines on the use of cookies and other trackers, 2020, available online at https://www.cnil.fr/sites/default/files/atoms/files/lignes_directrices_de_la_cnil_sur_les_cookies_et_autres_traceurs.pdf

delete such an identifier. Recent research shows that 87% of users (out of 2,230 users) retain at least one IP address for more than a month.[33]

- Additionally, we believe that it is a good practice to establish the requirements for a given technology, and not merely providing one technique (such as ID generation based on IP addresses) as the best practice in such general and high-level guidelines as the ones discussed here.

8. Le novità in materia di informativa
8.1 Le informazioni da rendere in conformità al Regolamento

"È inoltre necessario fornire informazioni su come le persone fisiche possono esercitare tutti i diritti previsti dal Regolamento, incluso quello di avanzare una richiesta di accesso e di proporre un reclamo a un'Autorità di controllo."

"It is also necessary to provide information on how individuals can exercise all the rights provided for by the Regulation, including the right to make an access request and to lodge a complaint with a supervisory authority."

- Indeed, information on the means to exercise all the rights, as well as information on data controllers, names of trackers, their purposes and other types of information need to be presented to the users in an accessible manner. We have collected all such requirements in section 5.4 (p.109) of our recent publication.[34]
- Additionally, as a general comment to the point 8.1? and as a best practice, we recommend that the consequences of the purposes of processing are defined and shown to the user. This is especially important for the purpose of "behavioral advertising" which entails profiling.

"[...] si ritiene inoltre che l'informativa, oltre che multilayer, e cioè dislocata su più livelli, possa ad oggi essere resa, eventualmente in relazione a specifiche necessità, anche per il tramite di più canali e modalità (cd. multichannel), in modo da sfruttare al massimo più dinamici e meno tradizionali ulteriori punti di contatto tra il titolare e gli interessati."

"(...)The information, as well as multilayer, i.e. spread over several levels, can now provided, possibly in relation to specific needs, also through multiple channels and methods (so-called multichannel), so as to make the most of more dynamic and less traditional additional points of contact between the owner and the interested parties".

- We welcome this practice, which is a novelty amongst DPAs, and attends to usability needs that needs to be accounted for in the design of information disclosure.

---

[33] Don't count me out: On the relevance of IP addresses in the tracking ecosystem. Vikas Mishra, Pierre Laperdrix, Antoine Vastel, Walter Rudametkin, Romain Rouvoy and Martin Lopatka. Proceedings of the 2020 edition of The Web Conference (WWW 2020).
[34] Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. Cristiana Santos, Nataliia Bielova and Célestin Matte.*International Journal on Technology and Regulation, 2020.*

8.2 The need for integration of the information to be communicated to users

"*Ci si riferisce al fatto che non esiste ancora, ad oggi, un sistema universalmente accettato di codifica semantica dei cookie e degli altri strumenti di tracciamento che consenta di distinguere oggettivamente, ad esempio, quelli tecnici dagli analytics o da quelli di profilazione, se non basandosi sulle indicazioni rese dal titolare stesso nella privacy policy."*

"*There is still no universally accepted system of semantic coding of cookies and other tracking tools that allows to objectively distinguish, for example, technical ones from analytics or profiling ones, if not based on the information provided by the owner himself in the privacy policy*."

- We agree that self-declaration of the purposes by the websites does not suffice to assure whether a cookie and other trackers are necessary to the provision of a service a user explicitly requested.
- In our recent study,[35] we found that "*12.85% of third-party cookies have a corresponding cookie policy where a cookie is even mentioned*" and that "*cookie policies do not comply with the purpose specification principle in 95% of cases*". In practice, cookie descriptions are often mixed with other text, which makes it hard to extract them, and are also formulated in a non specific and ambiguous way.
- We propose that **each cookie and tracking technology should have only one standard purpose and a legal basis applied to it**. Such standard description of each cookie could be represented in a structured table that enables automatic large scale auditing of cookies and other trackers. We have expressed this opinion in our feedback to the public consultation of the CNIL in February 2020.[36] We claim that the positioning of cookies in a table signifies best how cookie purposes can be "*clearly expressed and revealed*". The Belgian, French and UK DPA websites present cookie purposes inside of tables which include, for example: name, expiry date, content and purpose of cookies. We posit that this would be possible by a standardization of a purpose per cookie (being explicit, specific and legitimate, as per the purpose specification principle).[37]
- A semantic coding could be foreseen. Purposes of cookies and other similar technologies need to be pre-defined and modeled using ontologies that allow reasoning about purposes, inclusions, implications and generalisations. Such standardized approaches would serve to minimize legal uncertainty. Additionally, we recommend that a structured machine-readable representation of the purpose of trackers is proposed. Such machine-readable descriptions (1) allow a direct visual spotting of each purpose, and (2) enables an automatic, large-scale auditing of tracker descriptions for compliance and transparency concerns.

---

[35] On Compliance of Cookie Purposes with the Purpose Specification Principle, Imane Fouad, Cristiana Santos, Feras Al Kassar, Nataliia Bielova and Stefano Calzavara. *International Workshop on Privacy Engineering (IWPE 2020)*

[36] M. Toth, N. Bielova, C. Santos, V. Roca, and C. Matte. Contribution to the public consultation on the CNIL's draft recommendation on "cookies and other trackers", 2020. Research report, https://hal.inria.fr/hal-02490531

[37] Article 29 Working Party, "Opinion 03/2013 on Purpose Limitation (WP203).

“il Garante intende richiamare i titolari che facciano impiego di tali strumenti alla necessità di rendere manifesti, mediante apposita, opportuna integrazione dell’informativa, almeno i criteri di codifica degli identificatori adottati da ciascuno. Tali criteri potranno, inoltre, a richiesta, costituire oggetto di comunicazione all’Autorità, quale strumento di ausilio alle attività di carattere istruttorio che saranno intraprese con riguardo al fenomeno in considerazione.”

“the Guarantor intends to recall the owners who use these tools to the need to disclose, by means of a specific, appropriate integration of the information, at least the coding criteria of the identifiers adopted by each”

- We invite the Authority to further elaborate on *the coding criteria of identifiers*.
- In our feedback[38] to the recommendation of the CNIL, we propose that **each tracker should be well identified, have only one standardized purpose, categories/types of data collected, list of data controllers and a legal basis applied to it**. We also posit the need for a standardized naming convention for trackers from a predefined vocabulary of names.

[38] M. Toth, N. Bielova, C. Santos, V. Roca, and C. Matte. Contribution to the public consulta- tion on the CNIL’s draft recommendation on ”cookies and other trackers”, 2020. Research report, https://hal.inria.fr/hal-02490531