Alain Bensoussan Avocats
Le droit du numérique et des technologies avancées
Le réseau Lexing vous informe - The Lexing Network informs you
JTIT Internationale n° 9 – mars 2015
Special international issue #9– March 2015

L'UTILISATION DES COOKIES

USE OF COOKIES

TOUR DU MONDE DE LA RECETTE JURIDIQUE DES COOKIES

▪ L'article 32-II de la loi du 6 janvier 1978 prévoit que, sauf exception, les cookies ou autres traceurs ne peuvent être déposés ou lus sur le terminal d'un internaute, tant que celui-ci n'a pas donné son consentement après avoir été préalablement informé.

▪ Si certains cookies et traceurs ne sont pas soumis à cette réglementation, la CNIL, qui procède à des contrôles à distance et vérifie ainsi le respect de l'ensemble de ses dispositions, a émis certaines recommandations spécifiques pour les cookies pour aider les professionnels à se mettre en conformité.

▪ Malgré ces éléments, beaucoup de sites n'ont pas intégré dans leurs pages le code permettant le blocage des cookies soumis au recueil du consentement, ces derniers s'affichant alors avant que l'internaute ait donné son accord.

▪ Pour la mise en conformité d'un site internet, il est donc recommandé de connaitre les préconisations de la CNIL et de suivre une démarche de mise en conformité précise.

▪ Voici donc la recette des cookies « à la française ». Qu'en est-il dans les autres pays?

Les membres du réseau Lexing® dressent un tableau de la situation actuelle à travers le monde.

A WORLD TOUR OF THE COOKIES LEGAL RECIPE

▪ *Under French law (Article 32-II of the French Data Protection Act of 6 January 1978), the general rule is that cookies or other tracers may be installed or read on the terminal of a user only if such user has given their consent after receiving relevant information. There are, however, some exceptions to this rule for certain types of cookies and tracers.*

▪ *To help websites to comply with the relevant rules, the French Data Protection Authority issued specific recommendations about cookies. Note that the CNIL has the power to conduct remote controls to verify compliance.*

▪ *It appears that many websites have not built in their web pages the code for blocking cookies prior to obtaining user consent and such cookies are thus activated before the Internet user gives their consent.*

▪ *To be fully compliant with French law, website operators are recommended to review carefully the recommendations of the CNIL and follow a precise compliance program.*

▪ *Here is the cookies recipe "à la française." What about the other countries?*

The Lexing® network members provide a snapshot of the current state of play worldwide.

A propos de Lexing®

Lexing® est le premier réseau international d'avocats technologues dédié au droit des technologies avancées.

Créé sur une initiative d'Alain Bensoussan, Lexing® permet aux entreprises internationales de bénéficier de l'assistance d'avocats alliant la connaissance des technologies, des métiers et du droit qui leur sont applicables dans leur pays respectifs.

About Lexing®

Lexing® is the first international network of lawyers dedicated to technology law.

Created on an initiative of Alain Bensoussan, Lexing® allows multinationals to benefit from the assistance of seasoned lawyers worldwide who each combines unique expertise in technology and industry with a thorough knowledge of law in their respective country.

CÉLINE AVIGON

Dans de nombreux pays dans le monde, les cookies constituent un enjeu important. Quelle est la législation en matière de cookies en Afrique du Sud ? Est-il nécessaire d'obtenir le consentement préalable de l'utilisateur ? Existe-il des exemptions ? Autant de questions essentielles qui seront abordées dans cet article de manière simple et concise :

Qu'est-ce que les cookies et à quoi servent-ils ?

▪ Les cookies sont des fichiers texte transférés par votre navigateur Web sur le disque dur de votre ordinateur. Ces fichiers contiennent des informations à propos de votre navigation sur Internet. Toutes les entreprises dans le monde utilisent des cookies pour comprendre le comportement en ligne de leurs clients et améliorer ainsi l'interactivité avec leur site.

▪ Vous avez peut-être déjà remarqué qu'après avoir recherché en ligne un produit spécifique sur un site, des publicités relatives à ce produit apparaissent ensuite sur les pages d'autres sites que vous visitez ultérieurement. Vous vous êtes sûrement demandé pourquoi. En fait, lorsque vous vous connectez à un site qui utilise des cookies et que vous revenez plus tard sur ce site, les cookies lui permettent de se « souvenir » de vous.

▪ Les cookies sont destinés à faciliter la navigation des internautes, car de cette façon vous n'avez pas besoin, par exemple, de vous connecter à chaque fois que vous visitez la même page. Vos visites en ligne sont ainsi personnalisées selon vos préférences.

Quels sont les différents types de cookies ?

▪ Il existe plusieurs types de cookies, et chacun collecte des informations différentes, pendant des durées différentes. Par exemple, les cookies de session sont supprimés de votre ordinateur à la fin de votre session en ligne, tandis que les cookies persistants restent sur votre ordinateur jusqu'à ce qu'ils atteignent leur date d'expiration.

La loi POPI s'applique-t-elle aux cookies ?

▪ Oui, car même si la loi sud-africaine sur la protection des données personnelles, la « POPI » **(1)** ne vise pas explicitement les cookies, ils tombent néanmoins dans son champ d'application puisqu'un cookie est susceptible de contenir des informations personnelles **(2)**. Les données personnelles traitées par les cookies sont donc bel et bien protégées par la POPI.

▪ La POPI a été adoptée en 2013, mais n'est pas encore entrée en vigueur **(3)**. Une fois ce texte effectif, le Régulateur de l'information **(4)** pourra émettre des règlements en vue d'encadrer l'utilisation de cookies. Dans l'ensemble, la POPI repose sur le principe d'« opt-out » (consentement implicite de l'internaute), mais il est fort probable que l'Afrique du Sud se mette au diapason de la directive européenne « vie privée » et imposent aux propriétaires de site Web de recueillir le consentement des internautes avant d'installer des cookies sur leurs ordinateurs.

Qu'est-ce que cela signifie pour mes données personnelles ?

▪ Les cookies enregistrent certaines informations personnelles que vous communiquez lors de vos visites sur le Web. Ces informations personnelles peuvent faire l'objet d'un traitement de données, dans le respect des conditions posées par la POPI.

▪ En règle générale, les cookies ne stockent pas les numéros de cartes de crédit et les numéros de compte, mais si tel est le cas, ils doivent protéger ces informations et les traiter en toute sécurité. Les cookies ne peuvent stocker que des informations obtenues à partir de votre navigateur Web, et ne peuvent pas accéder aux données contenues sur votre disque dur. En outre, les cookies sont des fichiers texte et ne peuvent pas transmettre de virus à votre ordinateur ou à votre appareil mobile.

REFERENCES

(1) Protection of Personal Information Act ("POPI"). Cf. par ex. « POPI Act – Protection of Personal Information » sur http://www.michalsons.co.za/popi-act-protection-of-personal-information/11105

(2) Pour une définition de « données personnelles » en Afrique du Sud, cf. par exemple « What is personal information? », par John Giles http://www.michalsons.co.za/what-is-personal-information

(3) Le président Jacob Zuma a promulgué la loi POPI en novembre 2013, mais la date d'entrée en vigueur de cette loi n'est pas encore fixée. Une fois cette date est déterminée, les entreprises bénéficieront d'une période d'un an pour se mettre en conformité.
Nous estimons que la POPI ne devrait pas entrer en vigueur avant mi-2015, ce qui accorderait aux entreprises jusqu'à mi-2016 pour s'y conformer (cf. « POPI Commencement Date or POPI Effective Date », http://www.michalsons.co.za/popi-commencement-date-popi-effective-date/13109).
Toutefois, il leur est vivement recommandé de commencer d'ores et déjà le processus de mise en conformité.

(4) Le Régulateur de l'information (« Information Regulator ») est une nouvelle autorité de contrôle instituée par la POPI. Il dispose de pouvoirs étendus d'enquête et de. Les personnes concernées pourront déposer plainte auprès de cette autorité, qui sera habilitée à prendre des mesures en leur nom. Il s'agit de l'équivalent sud-africain de la Cnil française. (« Information Regulator in South Africa http://www.michalsons.co.za/information-regulator-in-south-africa/13893)

Quid de la Directive européenne « vie privée » ?

▪ La directive européenne « vie privée » **(5)** (telle que modifiée par la directive 2009/136/CE) **(6)**) exige l'obtention préalable du consentement éclairé des internautes pour les cookies. En effet, selon l'article 5, paragraphe 3, de cette directive « le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu (…) une information claire et complète ».

▪ Certes, une directive européenne n'est pas une loi, mais en cas de non-respect, l'État membre concerné s'expose à des sanctions **(7)**. Dès lors, les États membres sont tenus de transposer les directives dans leur droit national. En outre, même si une entreprise n'est pas établie sur le territoire de l'Union européenne, ses clients peuvent, eux, l'être. Dans ce cas, l'entreprise étrangère doit nécessairement obtenir le consentement de ses clients européens avant d'utiliser des cookies. L'UE exige par ailleurs d'adopter une « opt-in », c'est-à-dire que les internautes doivent activement consentir à l'utilisation des cookies. Une exception existe toutefois pour les cookies qui sont « strictement nécessaires pour la fourniture d'un service demandé par l'utilisateur ». Comme nous l'avons vu plus haut, la position européenne se situe à l'opposé de la position sud-africaine actuellement en vigueur, qui ne nécessite pas l'obtention du consentement (« opt-out »).

(5) Directive 2002/58/CE du 12 juillet 2002 (« Directive vie privée et communications électroniques ») http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32002L0058&from=FR

(6) Directive 2009/136/CE du 25 novembre 2009 (http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32009L0136&from=FR)

(7) Cf. http://ec.europa.eu/atwork/applying-eu-law/implementation-monitoring/index_fr.htm

Quel est le cadre juridique actuellement applicable en matière de cookies ?

▪ En Afrique du Sud, il n'existe actuellement aucune loi réglementant spécifiquement l'utilisation des cookies. En revanche, l'article 51 de la loi sur les communications et les transactions électroniques (ECTA) **(8)** régit la protection des données personnelles électroniques. Cet article, qui contient des exigences similaires aux futures dispositions de la POPI, sera d'ailleurs abrogé dès l'entrée en vigueur de la POPI.

▪ Pour l'instant, certains sites Web affichent de fenêtres pop-up pour vous informer qu'ils utilisent des cookies et vous recommandent de quitter leur site si vous ne souhaitez pas que vos données soient enregistrées. D'autres sites, en revanche, vous demandent votre consentement avant de les installer. Vous avez également la possibilité de modifier les paramètres de votre navigateur pour les bloquer.

(8) Cf. « Guide to the ECT Act in South Africa » http://www.michalsons.co.za/guide-to-the-ect-act/81

A quoi sert une politique de confidentialité ?

▪ La politique de confidentialité **(9)** est un document, facilement accessible, où vous pouvez savoir si le site que vous visitez utilise des cookies, et pourquoi il les utilise. Le bon reflexe est de systématiquement consulter ce document.

▪ Si vous êtes propriétaire d'un site Web qui utilise des cookies et recueille les données personnelles des utilisateurs, vous devez disposer d'une politique de confidentialité. Les internautes accordent une grande importance à leurs données personnelles. Une politique de confidentialité vous permet les informer de la manière dont vous protégez leurs données, et de gagner ainsi leur confiance.

(9) Cf. « Privacy Policy (for your customers or employees) » http://www.michalsons.co.za/privacy-policy-3/2501

Je suis propriétaire d'un site Web, que dois-je faire ?

▪ Si vos activités couvrent aussi bien l'Afrique du Sud que l'Union européenne, vous pouvez décider d'obtenir d'ores et déjà le consentement des internautes avant d'utiliser des cookies, quand bien même cette exigence ne s'applique pas encore en Afrique du Sud. Dans le cas où vos cookies collecteraient des numéros de compte, veuillez à bien mettre en œuvre des mesures de sécurité appropriées pour en garantir la protection, cet aspect étant particulièrement pris en compte par la POPI. Assurez-vous également d'afficher des fenêtres pop up alertant les visiteurs de votre site de l'utilisation de cookies.

▪ Le droit sud-africain étant appelé à évoluer prochainement en matière de cookies, il est conseillé de rester vigilant et de suivre régulièrement l'actualité législative.

OLIVIA SMITH

What is the cookie law in South Africa? Many people ask us because the law relating to cookies is such a big issue in many other countries. Do you need to get a user's (aka data subject's) consent before using cookies? Are there any specific regulations?

***What are cookies and why are they used**?*

▪ *Cookies are text files transferred from your browser to your computer's hard drive. They store information about your activity on a browser. Companies worldwide use cookies to monitor customer behaviour and to improve interactivity with a website.*

▪ *You will notice when you search for a specific product, ads relating to that product appear on other sites you visit. When you log into a website that uses cookies and later re-visit it, the cookies allow the website to 'remember' you.*

▪ *Cookies make your life as a website user much easier because you do not have to log in every time you visit the same page. Your online experiences will be personalized to your preferences.*

Types of cookies

▪ *There are different types of cookies saving different information and for different periods of time. Period cookies are deleted at the end of a web sessions, while persistent cookies have a pre-determined expiry date and will appear until the expiry date is reached.*

Does POPI apply?

▪ *POPI **(1)** does not explicitly mention cookies, but because a cookie can contain personal information **(2)**, POPI applies. The personal information that is processed using cookies will be protected by POPI.*

▪ *Once POPI commences **(3)**, the Information Regulator **(4)** may publish regulations to regulate the use of cookies in South Africa. Generally speaking, POPI is an opt-out law, but South Africa will probably follow the EU ePrivacy Directive and require the user (or data subject) to consent to a website owner using cookies.*

What about my personal information?

▪ *Cookies store certain personal information you provide on a website. This personal information can be processed if done so in accordance with the conditions of POPI.*

▪ *Cookies do not generally store credit card information and account numbers but if they do the information must be protected securely. Cookies only store information from your browser, they cannot access data on your hard drive. Cookies are text files that cannot transfer viruses to your computer or mobile device.*

REFERENCES

(1) Protection of Personal Information Act ("POPI"). See e.g. "POPI Act – Protection of Personal Information" on http://www.michalsons.co.za/popi-act-protection-of-personal-information/11105

(2) For a definition of "Personal Data" in South Africa see "What is personal information?", by John Giles (http://www.michalsons.co.za/what-is-personal-information)

(3) President Jacob Zuma signed the POPI Act into law in November 2013, but the actual commencement date of the Act is still to be determined. Once that date is set, businesses will have a one grace year to comply with the legislation.
We estimate that the POPI Act commencement date will probably only be in mid 2015. The one year grace period will then run from then, until mid 2016 (See "POPI Commencement Date or POPI Effective Date", http://www.michalsons.co.za/popi-commencement-date-popi-effective-date/13109). But this does not mean that you should not already be starting the process of complying with POPI.

(4) The Information Regulator is a new regulator that has been created by the Protection of Personal Information Act. It has extensive powers to investigate and fine responsible parties. Data subjects will be able to complain to the Information Regulator and the Information Regulator will be able to take action on behalf of data subjects. It is the South African equivalent of the Information Commissioner in the UK. ("Information Regulator in South Africa" http://www.michalsons.co.za/information-regulator-in-south-africa/13893)

EU ePrivacy Directive

▪ *The EU ePrivacy Directive* ***(5)*** *(as amended by Directive 2009/136/EC* ***(6)****) requires a data subject to give prior informed consent. EU ePrivacy Directive Article 5(3) says, "the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information"*

▪ *The Directive is not a law but failure to follow the directive will lead to action taken against the Member state* ***(7)****. Member states must implement the directive into local laws. Even if a business is not in the EU their customers might be. They must get their clients consent to use cookies. The EU requires data subjects to opt-in to the use of cookies. However, you do not need to get consent for cookies that are "strictly necessary for the delivery of a service requested by the user". This is contrary to the current South African position where consent is not needed.*

(5) Directive 2002/58/EC of 12 July 2002 (Directive on privacy and electronic communications) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN

(6) Directive 2009/136/EC of 25 November 2009 (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0136&from=EN)

(7) See http://ec.europa.eu/atwork/applying-eu-law/implementation-monitoring/index_en.htm

South African cookie law position?

▪ *In South Africa, there is currently no law regulating the use of cookies. But section 51 of the Electronic Communications and Transactions Act (ECTA)* ***(8)*** *governs the protection of electronic personal information. This provision has similar requirements to what is required under POPI and POPI will repeal it.*

▪ *Some websites have pop-ups informing you that they use cookies and state that if you do not want information saved, you should leave the website. Others require your specific consent before proceeding. You can also edit your browser settings to block the use of cookies.*

(8) See "Guide to the ECT Act in South Africa" http://www.michalsons.co.za/guide-to-the-ect-act/81

Privacy Policy

▪ *Have you read the privacy policy* ***(9)*** *of the websites you visit? Do they mention the use of cookies? Find out if they use cookies and what they use the cookies for. Companies usually refer to the use of cookies in their privacy policy and these privacy policies should be readily available to users.*

▪ *If you are a owner of a website that uses cookies and collects personal information about the data subjects, you need a privacy policy. Personal information is important to people and clients will feel safe knowing you are protecting their information. A privacy policy can help you achieve this trust. You should inform your clients of how you secure information they have entrusted to you.*

(9) See "Privacy Policy (for your customers or employees)" http://www.michalsons.co.za/privacy-policy-3/2501

What you can do as an owner of a website?

▪ *If you operate in South Africa and the EU, you might decide to get consent to use cookies even though this is currently not required in South Africa. If your cookies are storing account numbers you must implement security measures to protect the information. Under POPI, the protection of account numbers is very important. If you are using cookies ensure that you have pop ups alerting visitors to your website that cookies are being used.*

▪ *Cookie law may be addressed in South Africa in the future and you need to keep updated with the latest laws on cookies.*

OLIVIA SMITH

▪ La règlementation européenne en matière de cookies a été transposée en droit belge par l'article 90 de la loi du 10 juillet 2012 portant de dispositions diverses en matière de communications électroniques, à **l'article 129 de la loi du 13 juin 2005 relative aux communications électroniques (1)**.

(1) Loi du 13 juin 2005 relative aux communications électroniques

▪ Le principe de « l'**opt-out** » - l'installation des cookies autorisée à priori, à charge pour l'internaute de s'y opposer en configurant son navigateur – a été remplacé par le principe, très théorique, de « **l'opt-in** ». Les sites web ont maintenant l'obligation d'obtenir le consentement préalable et informé des internautes avant d'installer un cookie sur leur ordinateur.

▪ Force est de constater que cette exigence très (trop) lourde n'est pas respectée en pratique. Tout au plus, les gestionnaires de site web affichent-ils une bannière attirant l'attention des internautes sur le fait que, par l'utilisation du site web, ils marquent leur accord sur l'installation des cookies. Si l'information de l'internaute s'est généralement améliorée, on est très loin d'un consentement préalable et informé.

(2) Groupe de travail « Article 29 », Document de travail n°02/2013 énonçant des lignes directrices sur le recueil du consentement pour le dépôt de cookies, 2-10-2013

▪ Inspirée par les guidelines du Groupe de travail « Article 29 » **(2)**, la Commission de Protection de la Vie Privée belge a rédigé un **projet de recommandation concernant l'utilisation des cookies (3)** et l'a soumis à consultation publique. Après un examen technique et juridique des notions utilisées, ce projet de recommandation liste les différentes catégories de cookies et envisage, pour chaque catégorie de cookies, si une exemption à l'obligation de consentement préalable est envisageable, quelles sont les conditions de légitimité des finalités du traitement opéré, quel devrait être le contenu du cookie, sa durée de conservation et les informations préalables à fournir au visiteur.

(3) CPVP, Projet de recommandation d'initiative soumises à enquête publique concernant l'utilisation des cookies, CO-AR-2012-004.

▪ Ce document complet et technique permettra, certes, d'interpréter les exigences juridiques **de manière plus cohérente avec la pratique des professionnels** du web. Le fait que ces recommandations s'écartent de manière nette du texte clair de la loi en ce qui concerne l'exigence de consentement préalable devrait toutefois inciter le législateur à changer son fusil d'épaule plutôt que de conserver un texte inapplicable et inappliqué.

JEAN-FRANÇOIS HENROTTE

▪ *European regulations regarding cookies have been transposed into Belgian law via Article 90 of the Law of 10 July 2012 on various provisions on electronic communications, in* ***Article 129 of the Electronic Communications Act of 13 June 2005 (1)****.*

(1) Belgian Electronic Communications Act of 13 June 2015 (in French)

▪ *Previously, the "****Opt-out****" approach prevailed — i.e. it was assumed that the use of cookies was authorized, leaving it to users to later object by configuring their browser. "Opt-out" has now been replaced by the very theoretical "****Opt-in****" approach. In other words, websites today are required to obtain the prior and informed consent of users before installing a cookie on their computer.*

▪ *But this (too) heavy requirement is clearly not applied in practice. At most, website operators display a banner informing Internet users about the fact that, by using their website, they agree to the use of cookies. While the information provided to users has generally been improved, we are far from obtaining users' prior and informed consent.*

(2) Article 29 Data Protection Working Party, Working Document 02/2013 providing guidance on obtaining consent for cookies, 02-10-2013

▪ *Taking its cue from the guidelines of the EU Article 29 Data Protection Working Party* ***(2)****, the Belgian Privacy Commission drafted a* ***recommendation paper (3) on the use of cookies*** *and submitted it to public consultation. After presenting a technical and legal review of the different concepts used, the draft recommendation lists the various categories of cookies and examines, for each category, if an exemption from the prior consent requirement is possible, what the legitimate purposes of foreseen data processing are, what the content and shelf life of the cookies should be and what previous disclosures to the visitor should be given.*

(3) CPVP, Projet de recommandation d'initiative soumises à enquête publique concernant l'utilisation des cookies, CO-AR-2012-004.

▪ *This comprehensive and technical paper will certainly help to apply the legal requirements in a* ***more consistent and practical way****. The fact that this paper stands aside and departs from the clear text of the law regarding the requirement of consent should, however, encourage the legislature to change its tune rather than sticking to an inapplicable and unapplied text.*

JEAN-FRANÇOIS HENROTTE

Panorama de la législation californienne en matière de « Do Not Track »

▪ L'État de Californie dispose depuis 2003 d'une loi sur la protection des données personnelles en ligne, plus connue sous le nom de « CalOPPA ». La CalOPPA a été amendée en septembre 2013 par le projet de loi AB370, et codifiée sous le §22575 (b), point 5 à 7, du Code des entreprises et des professions libérales de Californie **(1)**. Le nouveau texte est entré en vigueur le 1er janvier 2014. En mai 2014, le procureur général de Californie a publié des directives sur les meilleures pratiques permettant de se conformer à cette législation. **(2)**

▪ Aux termes de la CalOPPA, l'opérateur d'un site Web marchand, d'une application mobile ou de tout autre service en ligne qui collecte les données personnelles de personnes résidant dans l'État de Californie (« service en ligne ») est tenu de diffuser, de manière visible, une politique de confidentialité devant obligatoirement contenir certains renseignements, tels que les catégories de données personnelles collectées par l'opérateur ainsi que les catégories de tiers avec lesquels celui-ci est susceptible de partager ces données.

▪ L'amendement intervenu en 2013 complète la liste des renseignements devant être fournis en imposant à l'opérateur de mentionner également :

- si le service en ligne prend en compte la fonction « Do Not Track » **(3)** des navigateurs Web ; et
- si des tiers peuvent collecter des données sur les activités en ligne des internautes dans le temps et sur différents services en ligne.

Mention relative à la fonction « Do Not Track » (paragraphe (b)(5))

▪ Première mention rendue obligatoire par l'amendement de 2013 : un service en ligne doit indiquer la façon dont il gère la fonction « Do Not Track », ou toutes autres fonctions similaires, permettant aux internautes de signaler qu'ils ne souhaitent pas être « suivis » par les services qu'ils consultent.

▪ Il convient de noter que le paragraphe de la CalOPPA relatif à la fonction « Do Not Track » est assez succinct (il ne fait que quelques lignes), et que par conséquent l'intention du législateur n'est pas clairement définie, notamment concernant la définition et la portée exactes de la fonction « Do Not Track » et des fonctions similaires.

▪ Sans définition précise, il est ainsi délicat de bien appréhender cette disposition. Par exemple, le ciblage (« targeting ») des internautes qui en résulte doit-il s'entendre de manière restreinte ou bien générale ? Le « tracking » est-il limité à l''utilisation d'informations dans le cadre de publicité comportementale en ligne, ou inclut-il également les technologies de suivi exploitées pour d'autres finalités, pouvant être moins intrusives, telles que la détection de la fraude ?

(1) California Online Privacy Protection Act. Cf. http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=22.&article=

(2)https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf

(3) Le « Do Not Track » ou « DNT » (pouvant être traduit par : « Ne me tracez pas ») est un outil qui vous permet de signaler que vous ne souhaitez pas être « suivi » sur le Web. Lorsque vous activez la fonction « Do Not Track » de votre navigateur Web, celui-ci envoie un signal à tous les sites Web que vous visitez les informant que vous ne voulez pas être suivis. Les entreprises connaissent ainsi vos préférences en matière de suivi et, dans le cas où elles se sont engagées à respecter ces préférences, elles sont légalement tenues de les respecter le faire. Tous les navigateurs ne prennent pas en charge la fonctionnalité « Do Not Track ». Pour bénéficier de cet outil, vous devez donc vérifier que votre navigateur le propose, ou à défaut changer de navigateur. Cf. "What is "Do Not Track"? https://www.consumer.ftc.gov/articles/0042-cookies-leaving-trail-web

- *Dérogation apportée par le paragraphe (b)(7)* – Par dérogation au paragraphe (b)(5), le paragraphe (b)(7) permet à l'opérateur d'un service en ligne de satisfaire à obligation d'information en matière de « Do Not Track » simplement en insérant, de manière claire et visible, au sein de sa politique de confidentialité, un lien hypertexte dirigeant les internautes vers « une description du fonctionnement et des effets des programmes ou protocoles utilisés par l'opérateur permettant d'offrir ce choix aux internautes ». Autrement dit, les services en ligne ont possibilité de ne pas insérer de clause spécifique à la fonction « Do Not Track » à condition de fournir aux utilisateurs de leur service un autre moyen de désactiver les fonctionnalités de suivi.

Mention relative aux tiers (paragraphe (b)(6))

▪ La deuxième mention rendue obligatoire par l'amendement de 2013 concerne les mécanismes de suivi de tiers. Toutefois, si le paragraphe (b)(6) impose aux services en ligne de divulguer l'existence d'outils de suivi tiers, ils ne sont pas tenus pour autant de décrire la finalité pour laquelle ces tiers peuvent utiliser les informations ainsi recueillies. Les entreprises sont donc libres de décider de l'étendue des informations ou des explications qu'elles souhaitent communiquer à propos des activités des tiers qu'elles autorisent à collecter des informations sur leur service en ligne.

Mesures d'application

▪ L'amendement de 2013 ne contenant pas de nouvelles dispositions relatives à son application, les dispositions de la CalOPPA en la matière restent intactes : les opérateurs disposent donc de 30 jours pour corriger toute non-conformité à la CalOPPA qui leur serait notifiée, avant de s'exposer à des poursuites du procureur général de l'État de Californie. Les entreprises contrevenantes encourent une amende pouvant atteindre 2 500 $ par infraction.

Conclusion

▪ L'amendement de 2013 à la loi CalOPPA n'interdit pas l'utilisation des fonctionnalités de suivi. Il impose simplement aux opérateurs de services en ligne d'informer les internautes s'ils prennent en compte la fonction « Do Not Track » et si les fournisseurs de services tiers ont la possibilité de collecter les données personnelles des internautes au cours de leur visite sur ce service en ligne et de les suivre dans le temps et sur d'autres services en ligne.

FRANÇOISE GILBERT
&
JOANNE KIRK

An Overview of California's 'Do Not Track' Legislation

▪ *In September 2013, the Governor of California signed into law California Assembly Bill AB370, which amended the California Online Privacy Protection Act 2003 (CalOPPA)* ***(1)****. It became effective on January 1, 2014, codified as California Business & Professional Code §22575(b) 5 to (b) 7. Subsequently in May 2014, the California Attorney General published best-practice guidance on the legislation* ***(2)****.*

▪ *Under CalOPPA the operator of a commercial website, a mobile application or other online service that collects personal information of California residents ("Online Service") must conspicuously display a privacy policy that discloses specified information, including the categories of personally identifiable information that the operator collects and the categories of third-parties with whom the operator may share that information.*

▪ *The 2013 amendment requires two further disclosures to be provided in such privacy policies. These are:*

- *How the Online Service responds to a browser's do-not track signal* ***(3)*** *regarding the collection of personal information about online activities over time and across third party online services; and*
- *Whether third parties may collect information about online activities over time and across different online services.*

Subsection (b)(5) Do Not Track Disclosure

▪ *Under this provision, an Online Service is obliged to disclose how it responds to 'do not track' signals or 'other mechanisms that provide the consumers the ability to exercise choice…".*

▪ *However, the entire "do not track" section is only a few lines long. It is not clear what "do not track" or "other mechanisms that provide consumers the ability to exercise choice" are intended to mean or cover.*

▪ *Without a proper definition of "do not track", it is difficult to interpret this provision. For example, does "targeting" cover specific targeting or only general profile categories? Is "tracking" limited to the use of information in connection with online behavioral advertising, or does it also include the tracking technologies that are used for other purposes, that are less privacy intrusive, such as fraud detection?*

(1)http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=22.&article=

(2)https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf

(3) "Do Not Track" or "DNT" is a tool that allows you to express your preference not to be tracked across the web. Turning on Do Not Track through your web browser sends a signal to every website you visit that you don't want to be tracked. Companies then know your preference. If they have committed to respect your preference, they are legally required to do so. Some browsers already support Do Not Track. If you want to use Do Not Track, check to see if the browser you use offers it – or use a browser that does. (See "What is "Do Not Track"? https://www.consumer.ftc.gov/articles/0042-cookies-leaving-trail-web)

- Subsection (b)(7) - Safe Harbor. *This provision creates a safe harbor or an alternative to Subsection (b)(5). It provides that the operator of an Online Service may satisfy the 'do not track' disclosure requirement by providing a clear and conspicuous hyperlink in its privacy statement to "a description, including the effects, of any program or protocol the operator follows that offers the consumer that choice." In other words, it offers Online Services the ability not to disclose whether they respond to a yet-to-be-defined "do not track" signal by providing users of their service a method for opting-out of the tracking.*

Subsection (b)(6) - Third Party Tracking Disclosure

▪ *The other change brought by the enactment of the 2013 amendment focuses on third party tracking mechanisms. Under Subsection (b)(6), Online Services must only disclose the existence of third parties tracking tools. They are not required to describe the purpose for which the third parties may use the collected information. Essentially, it has been left to companies to decide the extent of the disclosures or explanation they want to provide about the scope of the activities of the third parties that they invite or allow to collect information on their Online Service.*

Enforcement.

▪ *The amendment does not contain new provisions regarding the enforcement of these amendments. The current enforcement provisions of CalOPPA remain untouched. Therefore operators subject to CalOPPA have 30 days to correct deficiencies after being notified of non-compliance before the Attorney General can take action. Companies can face fines of up $2500 per violation of CalOPPA.*

Conclusion

▪ *The 2013 amendment to CalOPPA does not prohibit tracking. It only requires that operators of Online Services disclose how they respond to a do-not-track signal, and whether third party service providers have the ability to collect personal information from individuals during their visit of that Online Service and follow that individual over time and on other Online Services.*

FRANÇOISE GILBERT
&
JOANNE KIRK

La recette française des cookies

▪ La loi française prévoit que, sauf exception, les cookies **(1)** ou autres traceurs ne peuvent être déposés ou lus sur le terminal d'un internaute, tant que celui-ci n'a pas donné son **consentement** après avoir été préalablement informé **(2)**.

▪ Les responsables de traitement qui mettent en œuvre des cookies ou autres traceurs doivent donc informer préalablement l'utilisateur et recueillir son consentement préalable. Les sites doivent en outre solliciter le consentement de l'utilisateur tous les **13 mois**, au maximum.

▪ Mais tous les cookies n'obéissent pas à cette règle. Dans sa **délibération n°2013-378 (3)**, la Cnil a émis certaines recommandations pour les cookies nécessitant de recueillir le consentement préalable.

▪ Même si les recommandations de la Cnil n'ont pas la même valeur qu'une loi ou un décret, elles définissent un état de l'art et ne sont donc pas dépourvues de valeur. Elles représentent les **bonnes pratiques** que doivent respecter les professionnels.

▪ La Cnil qui peut procéder des **contrôles à distance** vérifie le respect de l'ensemble de ses préconisations **(4)**. A cette fin elle analyse **(5)** :

- les types de cookies utilisés par le site web, leurs finalités et la connaissance par les éditeurs de site de la finalité de tous les cookies déposés ou lus depuis leur site ;
- les finalités des cookies utilisés, et l'existence de cookies sans finalité ;
- les modalités de recueil du consentement dans le cas où la finalité du cookie utilisé l'impose ;
- la visibilité, la qualité et la simplicité de l'information relative aux cookies ;
- les conséquences, en cas de refus de l'internaute d'accepter le dépôt des cookies nécessitant un consentement ;
- l'existence de la possibilité pour l'internaute de retirer son consentement à tout moment ;
- le respect de la durée de vie maximale des cookies et de la validité du consentement de l'internaute à 13 mois ;
- la sécurité des données, la présence de données sensibles, etc.

REFERENCES

(1) Également appelés « témoins de connexion », les cookies sont des traceurs déposés sur le disque dur d'un internaute par le serveur du site visité et qui permettent à celui qui les a déposés de reconnaître, d'une visite à une autre, un internaute grâce à un identifiant unique.
Ces cookies peuvent être utilisés à différentes fins : pour stocker le contenu d'un panier d'achat, pour enregistrer les paramètres de langue d'un site, ou encore pour faire de la publicité ciblée par l'analyse de la navigation. Cf. Céline Avignon, « La nouvelle recette des cookies à la française », Gaz. Pal. nos 287-288 des 14 et 15-10-2011.

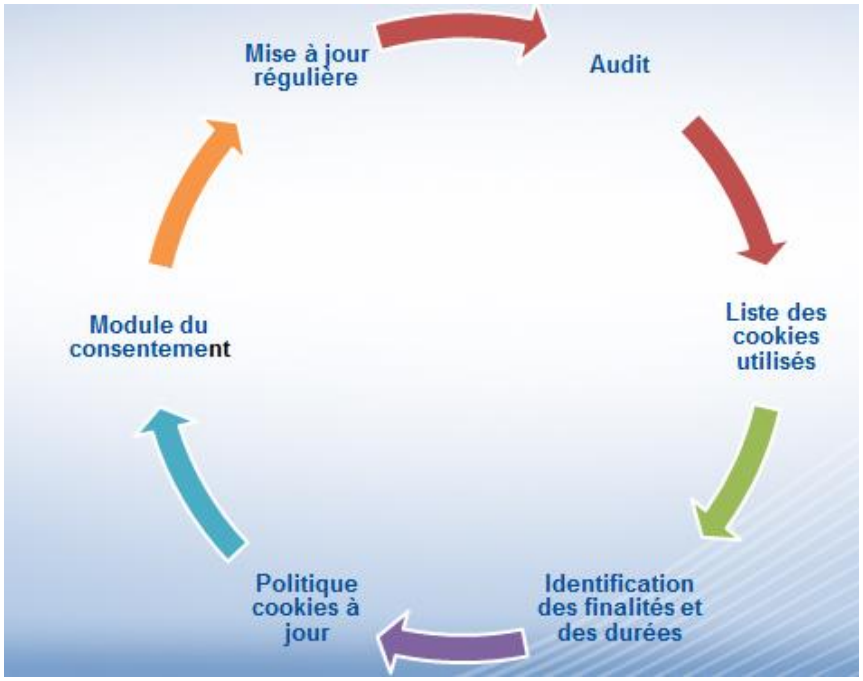
(2) Art. 32-II de la loi du 6 janvier 1978. Cet article transpose en droit français les principes contenus dans la directive européenne 2009/136/CE dite « paquet télécom », selon lesquels les internautes doivent être informés et donner leur consentement préalable à l'insertion de traceurs sur leur ordinateur. Certains traceurs, tels que les cookies techniques, sont toutefois dispensés du recueil de ce consentement Cf. « Le nouveau régime juridique des cookies: information et consentement », par Céline Avignon, emarketing.fr, 1-11, 2011.

(3) Délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux Cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978.

(4) La loi du 17 mars 2014 relative à la consommation modifie la loi Informatique et Libertés (art. 44) donne à la CNIL la possibilité de procéder à des contrôles en ligne et de constater à distance des manquements à la loi Informatique et Libertés.

▪ D'expérience, beaucoup de sites affichent **le bandeau** de recueil de consentement **(6)** ainsi qu'une politique cookies pour informer les internautes mais n'ont pas intégré dans les pages **le code** nécessaire pour bloquer les cookies soumis au recueil du consentement. Or, en l'absence de ce blocage, les cookies soumis au consentement s'affichent avant même que l'internaute n'ait donné son accord. En conséquence, cette vérification est essentielle dans le cadre dans le management de la conformité.

▪ **Pour conclure, si vous devez mettre en conformité un site internet, il est recommandé de mettre en œuvre la démarche suivante (7)** :



(5) Du 15 au 19 septembre 2014, la Cnil a mené, aux côtés de ses homologues européens, un audit des principaux sites internet européens, afin de dresser un état des lieux des pratiques en matière de cookies. Cette opération est appelée « Cookies Sweep Day ».
En outre, la Cnil a également annoncé qu'à compter du mois d'octobre 2014, elle procéderait au contrôle du respect des principes issus de sa recommandation relative aux cookies et autres traceurs de 2013. Cf. « Cookies : la Cnil annonce des contrôles sur la mise en œuvre de ses recommandations concernant les cookies et autres traceurs », Céline Avignon, ecommercemag.fr, 17-7,2014 et « Cookies sweep days : répétition générale avant le lancement de contrôles par la Cnil », Stratégie internet, n°186, Octobre-Novembre 2014).

(6) Cf. page d'explication du Bandeau cookie du site de la Cnil

(7) Sur son site la Cnil met à disposition de tous (internautes, webmasters, développeurs) « Cookieviz », un outil de visualisation qui identifie en temps réel les cookies qui transmettent des informations vous concernant à d'autres sites.

CÉLINE AVIGON

The French Cookie Recipe

▪ Under French law, the general rule is that cookies **(1)** or other tracers may be installed or read on the terminal of a user only if such user has given their **consent** after receiving relevant information **(2)**.

▪ Data controllers who want to use cookies and like should therefore first inform users and then collect their prior consent. Moreover, consent should be renewed at least every **13 months**.

▪ By and large, prior consent is thus the rule in France; but other specific rules can apply. To clarify the cookie consent rule, the French data protection authority, the CNIL, issued a series of recommendation in 2013.

▪ While the recommendations of the CNIL do not have the same value as a law or decree, they nonetheless give a clear picture of a state of the art and thus represent the **best practices** to be followed by businesses.

▪ In addition, the CNIL is empowered **(4)** to **carry out remote checks** to verify compliance with its recommendations **(5)**. In performing such checks, the French data protection watchdog will focus on:

- the types of cookies used by the website;
- the purposes of cookies used, whether website operators are aware of the purpose of all the cookies that are installed or read from their sites, and whether there are cookies with no purpose;
- how consent is obtained (if consent is required);
- the visibility, quality and simplicity of information given about cookies;
- the consequences in case a user refuses to consent to cookies;
- the possibility for users to withdraw consent at any time;
- the cookies maximum shelf live and 13-month validity period of the user consent;
- and a series of other points such as data security, sensitive data, etc.

REFERENCES

(1) Also known in French as "*témoins de connexion*", cookies are tracers placed on internet users' hard drives by the web hosts of the visited website. They allow the website to identify a single user across multiple visits with a unique identifier.
Cookies may be used for various purposes: building up a shopping cart, storing a website's language settings, or targeting advertising by monitoring the user's web-browsing. See. Céline Avignon, « La nouvelle recette des cookies à la française », Gaz. Pal. nos 287-288 des 14 et 15-10-2011.

(2) Art. II-32 of the French Data Protection Act of 6 January 1978. Such Article implements into French law the principles of EU Directive 2009/136/EC, the so-called "Telecom Package", under which internet users must be informed and provide their prior consent to the storage of cookies on their computer. Some tracers, such as functional cookies, are exempted from this consent rule. See « Le nouveau régime juridique des cookies: information et consentement », par Céline Avignon, emarketing.fr, 1-11, 2011.

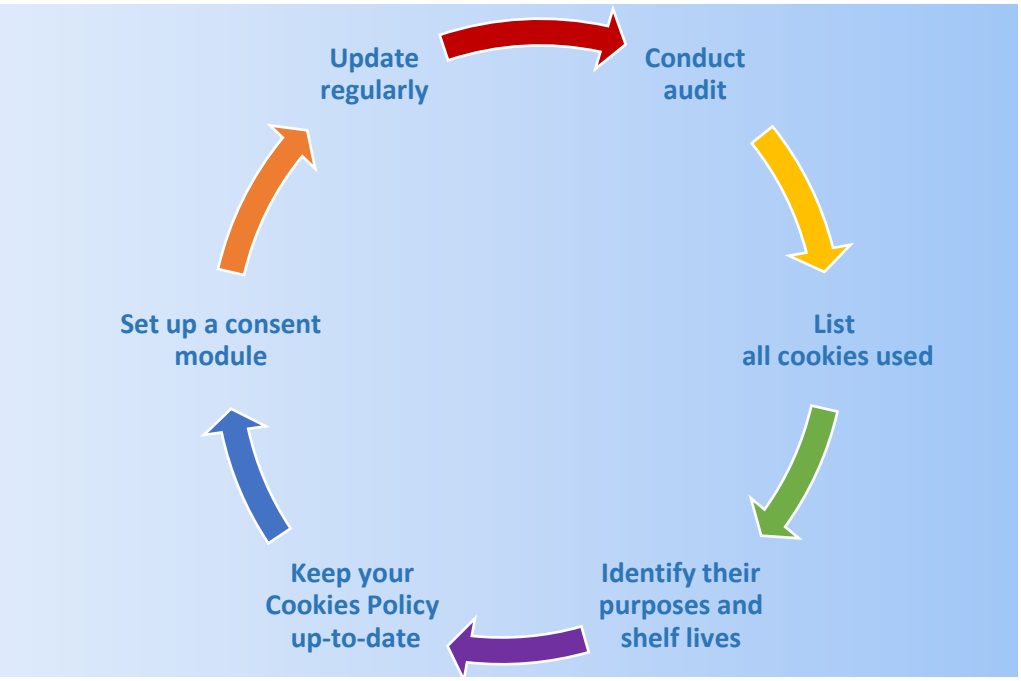
(3) Délibération No. 2013-378 of 5 December 2013 adopting a recommendation on Cookies and other tracers referred to in Article 32-II of the Act of 6 January 1978

(4) The Consumption Act of 17 March 2014 amended the Data Protection Act (art. 44)) to give the CNIL the power to make online inspections and identify breaches of the Data Protection Act.

(5) From 15 to 19 September 2014, the CNIL and its European counterparts carried out an audit of the main European websites in order to assess their practices with regard to cookies. This is

▪ From our experience, while many websites display **the consent banner (6)** and have a cookies policy to inform users, they do not all have implemented into their pages **the code** needed to block cookies prior to obtaining user consent. However, without this blocking code, cookies are activated even before the user has given their consent. An efficient compliance management should thus include a check of this aspect.

▪ **In conclusion, for your website to be cookies-compliant, it is recommended to follow the following legal recipe (7)**:



known as the "Cookie Sweep Day" operation.
In addition, the CNIL also announced that starting October 2014 it would begin auditing websites in France to verify compliance with the cookie provisions enshrined in its 2013 recommendation. See « Cookies : la Cnil annonce des contrôles sur la mise en œuvre de ses recommandations concernant les cookies et autres traceurs », Céline Avignon, ecommercemag.fr, 17-7,2014 and « Cookies sweep days : répétition générale avant le lancement de contrôles par la Cnil », Stratégie internet, n°186, Octobre-Novembre 2014).

(6) See page describing cookie consent banner on CNIL's website (« Bandeau cookie »).

(7) A tool called "Cookieviz " is available on the CNIL's website to help users, website operators, webmasters and developers to visualize in real time the cookies of a website.

CÉLINE AVIGON

▪ Les nouvelles technologies et les outils de publicité comportementale posent de nouveaux défis en matière de confidentialité et de sécurité des données. Parmi ces outils de marketing et de e-commerce figurent bien entendu les cookies.

▪ En Grèce, l'utilisation de cookies est encadrée par la loi. Aux termes de **l'article 170 de la loi 4070/2012** [transposant la directive communautaire sur les cookies (2009/136/CE) **(1)** et modifiant l'article 4 de la loi 3471/2006 (« Protection des données personnelles et la vie privée dans le secteur des télécommunications électroniques »)] **(2)**, le stockage d'informations sur le périphérique d'un utilisateur et l'accès à ces informations ne sont autorisés que si l'utilisateur a donné son **consentement éclairé**.

▪ Ce consentement peut être donné en utilisant les paramètres appropriés du navigateur Web ou d'une autre application.

▪ Les dispositions ci-dessus ne font pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques ou à un stockage ou à un accès techniques nécessaire pour la fourniture d'un service de la société de l'information, expressément demandé par l'utilisateur.

▪ **L'autorité hellénique de protection des données (3)** a récemment publié des **lignes directrices sur les cookies** destinées à préciser davantage le cadre légal. Elles abordent notamment les cas, exceptionnels, où aucun consentement n'est requis (en reprenant, en substance, l'avis 04/2012 du Groupe de travail de l'article 29 sur l'exemption de l'obligation de consentement pour certains cookies) **(4)**. Ces **dérogations** couvrent par exemple les cookies alimentés par l'utilisateur, les cookies de sécurité centrés sur l'utilisateur, les cookies de session créés par un lecteur multimédia, les cookies d'authentification, les cookies de personnalisation de l'interface utilisateur, les cookies de session d'équilibrage de charge, et les cookies de modules sociaux de partage de contenu.

▪ En revanche, s'agissant des **cookies de mesure d'audience et de publicité** (cookies d'origine et cookies tiers), les lignes directrices de l'autorité hellénique de protection des données précisent qu'ils tombent hors du champ des exemptions mentionnées ci-dessus, et que par conséquent le **consentement préalable de l'utilisateur est nécessaire**.

▪ L'autorité hellénique de protection des données reconnait toutefois que la question des cookies de mesure d'audience est complexe et nécessite de procéder à un nouvel examen plus approfondi.

▪ Pour finir, elle souligne l'importance de mettre en place un mécanisme simple et facile permettant aux internautes de refuser la collecte de leurs données (« **opt-out** »).

(1) Directive 2009/136/CE du 25-11-2009

(2) Loi 3471/2006 (traduction anglaise)

(3) Autorité hellénique de protection des données (site Web)

(4) Groupe de travail « Article 29, » Avis 04/2012 sur l'exemption de l'obligation de consentement pour certains Cookies (WP 194), 07-06-2012

GEORGE A. BALLAS

▪ *The implementation of new technologies and tools for the needs of behavioural advertising poses new data privacy and security challenges; cookies are such marketing and e-commerce tools.*

▪ *In Greece the use of cookies is regulated by law. According to* ***Article 170 of Law 4070/2012*** *[implementing EU Cookies Directive (2009/136/EC)* ***(1)*** *and amending Article 4 of Law 3471/2006 ("Protection of personal data and privacy in the electronic telecommunications sector")]* ***(2)****, the storage of information on or the access to information already stored on a device of a user is permitted only if the user has provided his* ***informed consent****.*

(1) Directive 2009/136/EC of 25-11-2009

(2) Law 3471/2006 (English translation)

▪ *Such consent can be expressed by using the appropriate settings of a browser or other application.*

▪ *The above does not prevent any technical storage or access for the sole purpose of carrying out a transmission of a communication over an electronic communications network or any technical storage or access which is necessary for the provision of an information society service, which has been explicitly requested by the user.*

▪ *Recently published* ***Guidelines on cookies*** *by the* ***Hellenic Data Protection Authority*** *(DPA)* ***(3)*** *attempt to further explain the relevant provision. They refer to exceptions where no consent is required (basically reproducing the Article 29 Working Party Opinion 04/2012 on Cookie* ***Consent Exemption (4)****); such are the cases of "user-input" cookies, user-centric security cookies, multimedia player session cookies, authentication cookies, UI customization cookies, load balancing session cookies, social plug-in content sharing cookies.*

(3) Hellenic Data Protection Authority (website)

(4) Article 29 Data Protection Working Party, Opinion 04/2012 on Cookie Consent Exemption (WP 194), 07-06-2012

▪ *Special reference is also made to* ***"web analytics" cookies and "online advertising" cookies*** *(first-party cookies and third-party cookies), which according to the DPA Guidelines are not included in the above exceptions and therefore* ***prior consent is required****.*

▪ *The DPA recognizes though the need to further review and discuss the issue of "web analytics" cookies.*

▪ *It is also noted that a user friendly mechanism to* ***opt-out*** *must be in place.*

GEORGE A. BALLAS

▪ Le 8 mai 2014, l'autorité italienne de protection des données **(1)**, le *Garante*, a publié un règlement présentant des « modalités simplifiées pour la fourniture d'informations et l'obtention du consentement en matière de cookies » **(2) (3)**. Ce règlement prendra effet bientôt, à compter du 2 juin 2015.

▪ La réglementation italienne opère une distinction entre **deux principaux types de cookies** : les cookies techniques et les cookies de profilage **(4)**.

- Les **cookies techniques** sont utilisés exclusivement pour effectuer « la transmission d'une communication par la voie d'un réseau de communications électroniques, ou dans la mesure où cela est strictement nécessaire au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par la partie contractante ou l'utilisateur ». Ils comprennent eux-mêmes plusieurs catégories : les cookies de navigation ou de session nécessaires pour surfer sur un site donné, les cookies fonctionnels qui permettent l'activation de certains paramètres (par ex., la langue du site), ou encore les cookies analytiques qui recueillent des informations globales sur le nombre de visiteurs et la raison de leurs visites sur un site Web. Les cookies techniques ne nécessitent pas le consentement préalable des internautes.
- Les **cookies de profilage** sont utilisés pour « pour envoyer des messages publicitaires personnalisés correspondant aux préférences indiquées par l'utilisateur lors de sa navigation ». Ce type de cookie est considéré comme « très intrusif » et requiert donc de recueillir le consentement des internautes.

▪ Les internautes doivent être informés de l'existence de cookies de profilage selon une procédure à deux étapes : tout d'abord par une mention d'information succincte (sous forme de bandeau), puis par une notice d'information plus complète **(5)**.

▪ S'agissant de la **mention d'information succincte**, qui doit apparaître de manière visible lors de la première visite de l'internaute sur le site, elle doit informer l'internaute :

- que le site utilise des cookies de profilage dans le but d'envoyer des messages publicitaires ciblés selon les préférences de navigation de l'internaute ;
- que le site permet également le dépôt de cookies tiers (le cas échéant) ;
- qu'il peut accéder, en cliquant sur le lien fourni, à une notice d'information complète apportant des précisions sur les cookies techniques et de mesure d'audience, ainsi que sur les outils permettant de les activer ou de les désactiver ;
- qu'il peut refuser l'installation de tout type de cookies en se rendant sur la notice d'information ;
- que le fait de poursuivre sa navigation sur le site, en se rendant sur une autre page du site ou cliquant sur un élément du site (par exemple une image ou un lien), vaut accord à l'installation de cookies.

REFERENCES

(1) Garante per la protezione dei dati personali: www.garanteprivacy.it

(2) Règlement sur les cookies « « Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie, disponible en italien et en anglais sur le site Web du Garante.

(3) Les dispositions relatives à l'utilisation de cookies s'appliquent également aux dispositifs similaires qui permettent l'identification des utilisateurs ou de leurs terminaux, tels que les pixels invisibles (balises Web, web bugs, GIF clair).

(4) Cookie "tecnici" e cookie "di profilazione"

(5) Banner contenente informativa breve e informativa estesa.

▪ En pratique, cela signifie que deux choix se présentent à l'internaute lors de l'apparition du bandeau : poursuivre sa navigation sur le site (et donc consentir par là-même à la dépose de cookies) ou bien cliquer sur le lien pour accéder à la **notice d'information complète**. Outre les renseignements devant être transmis aux personnes concernées et énumérés dans le Code de protection des données **(6)**, cette dernière doit inclure une description détaillée de tous les cookies utilisés par le site, et offrir aux internautes la possibilité de sélectionner les cookies qu'ils souhaitent accepter et ceux qu'ils souhaitent, au contraire, refuser.

▪ Dans le cas où le site utiliserait des cookies tiers, un lien doit être inséré vers le site Web de ces tierces parties, où figureront toutes les informations détaillées concernant leurs cookies, ainsi que la possibilité de les refuser.

▪ En outre, les sites Web utilisant des cookies de profilage doivent déclarer les traitements effectués, conformément à l'article 37.1 du Code de protection des données.

▪ Consciente des conséquences considérables que ce règlement engendrera pour les acteurs du secteur, le Garante a été décide de fixer son **entrée en vigueur au 2 juin 2015**.

▪ Les contrevenants au Règlement sur les cookies seront passibles d'**amendes**, définies dans le Code de protection des données, dont le montant varie en fonction de la nature de l'infraction :

- Notice d'information insuffisante : de 6.000 à 36.000 € (art. 161) ;
- défaut de déclaration : de 20.000 à 120.000 € (art. 163) ;
- installation des cookies sans le consentement de l'utilisateur : de 10.000 à 120.000 € (art. 162).

▪ Enfin, il est important de se rappeler que le fait de procéder au traitement des données à caractère personnel sans le consentement de l'utilisateur expose également à des **sanctions pénales**, prévues à l'article 167 du Code, pouvant aller de six mois à trois ans. Par conséquent, différentes sanctions peuvent être infligées, la différence étant que les amendes administratives visées aux articles 161, 162 et 163 du Code peuvent être prononcées par l'autorité italienne de protection des données, tandis que les sanctions pénales ne peuvent être décidées que par les tribunaux dans le cadre de procédures pénales.

(6) Article 13 du Code italien de protection des données (« Codice in materia di protezione dei dati personali ») (version italienne et version anglaise).

RAFFAELE ZALLONE

REFERENCES

▪ *On May 8, 2014, the Italian Authority **(1)** published a regulation, "Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies" **(2)** **(3)**, which shall become effective as of June 2, 2015.*

▪ *The Italian regulation divides cookies in **two categories**, technical cookies and profiling cookies **(4)**.*

- ***Technical cookies** are those used exclusively to carry out "the transmission of a communication on an electronic communications network, or insofar as this is strictly necessary to the provider of an information society service that has been explicitly requested by the contracting party or user to provide the said service." They can be split into several sub-categories: browsing or session cookies, needed to allow navigation in a given website, functional cookies, which allow certain settings (i.e., language) and analytic cookies that collect aggregate information on the number of visitors and the pattern of visits to a website. These cookies do not require consent of the users.*
- *The second category is **profiling cookies**, defined as those used "to send ads messages in line with the preferences shown by the user during navigation." These cookies are considered to be "highly invasive" and for them consent of the users is required.*

▪ *The information notice regarding the use of profiling cookies must be given in two ways **(5)**: first of all by means of a summarized notice, which must be clearly visible to the user when opening the page for the first time.*

▪ *This **summary notice** must include the following detail:*

- *That the website uses profiling cookies to send advertising messages in line with the user's online navigation preferences;*
- *If applicable, that the website also allows the sending of third-party cookies;*
- *A clickable link to the extended information notice (see below), where information on technical and analytics cookies must be provided along with tools to select the cookies to be enabled;*
- *That the user may refuse to consent to the installation of whatever cookies on the extended information notice;*
- *That if the user continues browsing by accessing any other section or selecting any item on the website (e.g., by clicking a picture or a link), he/she signifies his/her consent to the use of cookies.*

(1) Garante per la protezione dei dati personali: www.garanteprivacy.it

(2) Cookie Regulation "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie, available in Italian and in English on the Garante website

(3) The provisions on the use of cookies also apply to similar tools such as web beacons, web bugs, clear GIFs or others, which allow identifying users or terminals.

(4) Cookie "tecnici" e cookie "di profilazione"

(5) Banner contenente informativa breve e informativa estesa.

▪ *This means, in practice, that the user has two initial choices: continue navigation on the site, which expresses consent, or use the link and access the full-fledged information notice. This* ***extended information notice*** *must include all the elements required under the law* ***(6)****, the detailed description of all cookies and users must have the option to pick and choose which ones to accept and which ones to refuse.*

▪ *If third-party cookies are used by the site, there must be a link to the website of these third parties, which must include all the details of their cookies as well as the option to refuse them.*

▪ *Websites using profiling cookies must notify this processing, as provided for by Section 37.1 of the Law.*

▪ *The implementation of the Regulation has been set at* ***June 2, 2015****, in the light the considerable impact this regulation will have on the IT sector.*

▪ *Failure to comply with the regulation will result in* ***fines****, which vary depending on the violation:*

- *Failure to give adequate notice is punished with fine ranging from EUR 6,000 to EUR 36,000 (sec. 161 of the Law);*
- *Failure to notify carries a sanction from EUR 20,000 to EUR 120,000 (sec. 163 of the Law);*
- *Installation of cookies without the user consent calls for a fine ranging from EUR 10,000 to EUR 120,000 (sec. 162 of the law).*

▪ *In addition, it is important to remember that processing personal data without consent also calls for the* ***criminal sanctions*** *provided for by Section 167 of the Law, ranging from six months to three years term. Therefore, these general sanctions might be applied, the difference being that the administrative fines indicated above and set for by Section 161, 162, and 163 may be levied by the Authority, while criminal sanctions may only be determined by ordinary courts in criminal proceedings.*

(6) Section 13 of the Italian Personal Data Protection Code ("Codice in materia di protezione dei dati personali") (Italian version and English version).

RAFFAELE ZALLONE

PAYS / COUNTRY	CABINET / FIRM	CONTACT	TELEPHONE	EMAIL
Afrique du Sud *South Africa*	Michalsons Attorneys	Lance Michalson John Giles	+27 (0) 21 300 1070	lance@michalsons.co.za john@michalsons.co.za
Allemagne *Germany*		Tim Christopher Caesar		
Argentine *Argentina*	Estudio Millé	Antonio Millé Rosario Millé	+ 54 11 5297 7000	antonio@mille.com.ar rosario@mille.com.ar
Belgique *Belgium*	Philippe & Partners	Jean-François Henrotte	+ 32 4 229 20 10	jfhenrotte@philippelaw.eu
Brésil *Brazil*	Melchior, Micheletti e Amendoeira Advogados	Silvia Regina Barbuy Melchior	+ 55 113 8451511	melchior@mmalaw.com.br
Canada *Canada*	Langlois Kronström Desjardins	Jean-François De Rico	+1 418 650 7923	jean-francois.derico@lkd.ca
Chine *China*	Jade & Fountain PRC Lawyers	Jun Yang	+86 21 6235 1488	jun.yang@jadefountain.com
Colombie *Colombia*	Marrugo Rivera & Asociados	Ivan Dario Marrugo Jimenez	+57 1 4760798	imarrugo@marrugorivera.com
Espagne *Spain*	Lexing Spain	Marc Gallardo	+ 34 93 476 40 48	marc.gallardo@lexing.es
États-Unis *USA*	IT Law Group	Françoise Gilbert	+ 1 (650) 804 1235	fgilbert@itlawgroup.com
France *France*	Alain Bensoussan-Avocats	Alain Bensoussan	+33 1 82 73 05 05	paris@alain-bensoussan.com
Grèce *Greece*	Ballas, Pelecanos & Associates L.P.C.	George A. Ballas	+ 30 210 36 25 943	central@balpel.gr
Israël *Israel*	Livnat, Mayer & Co.	Russell D. Mayer	+972 2 679 9533	mayer@lmf.co.il
Italie *Italy*	Studio Legale Zallone	Raffaele Zallone	+ 39 (0) 229 01 35 83	r.zallone@studiozallone.it
Liban *Lebanon*	Kouatly & Associates	Rayan Kouatly	+ 961 175 17 77	info@kouatlylaw.com
Luxembourg *Luxembourg*	Philippe & Partners	Jean-François Henrotte	+ 32 4 229 20 10	jfhenrotte@philippelaw.eu
Mexique *Mexico*	Langlet, Carpio y Asociados, S.C.	Enrique Ochoa De Gonzälez Argüelles	+ 52 55 25 91 1070	eochoa@lclaw.com.mx
Nouvelle-Calédonie *New Calédonie*	Cabinet Franck Royanez	Franck Royanez	+ 687 24 24 48	fr.avocat@cabinetroyanez.com
Norvège *Norway*	Føyen Advøkatfirma DA	Arve Føyen	+ 47 21 93 10 00	arve.foyen@foyen.no
Royaume-Uni *UK*	Preiskel & Co LLP	Danny Preiskel	+ 44 (0) 20 7332 5640	dpreiskel@preiskel.com
Portugal *Portugal*	Alves Pereira & Teixeira de Sousa	João P. Alves Pereira	+ 351 21 370 01 90	jpereira@alvespereira.com
Suisse *Switzerland*	Sébastien Fanti	Sébastien Fanti	+ 41 (0) 27 322 15 15	sebastien.fanti@sebastienfanti.ch
Tunisie *Tunisia*	Younsi & Younsi International Law Firm	Yassine Younsi	+216 71 34 65 64	cabinetyounsi_younsi@yahoo.fr

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris, président : Alain Bensoussan
Directeur de la publication : Alain Bensoussan - Responsable de la rédaction : Isabelle Pottier
Diffusée uniquement par voie électronique - gratuit -
ISSN 1634-0701
Abonnement à partir du site : http://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-juristendance/