

---

## ACTUALITÉS JANVIER 2022

---

### 1. Projet de loi Monégasque relative à la protection des données personnelles

Un projet de loi venant réformer la protection des informations nominatives a été déposé devant le Conseil National, fin décembre 2021.

La CCIN lui a consacré un article dans le cadre de la Journée Internationale de la Protection des Données qui a eu lieu le 28 janvier 2022.

Le texte, qui est encore en l'état de projet, est disponible sur le site du Conseil National en cliquant [ICI](#)

Lors de la Séance Publique du Conseil National du 31 janvier 2022 ce projet de loi a été renvoyé devant la Commission pour la Développement du Numérique.

### 2. Protocole du Comité des Ministres du Conseil de l'Europe

Un second protocole, additionnel à la Convention sur la cybercriminalité (Convention de Budapest dédiée à la lutte contre la criminalité informatique et sur internet) a été adopté par le Comité des Ministres du Conseil de l'Europe.

Ce protocole prévoit l'incrimination des actes de nature raciste et xénophobe, commis pas le biais de systèmes informatiques. Il constitue également une base juridique pour la divulgation des informations relatives à l'enregistrement des noms de domaine et la coopération directe avec les fournisseurs de services pour les informations sur les abonnés, tout en prévoyant des garanties au regard du respect de la vie privée et du traitement des données à caractère personnel.

A noter que son champ d'application dépasse celui des seules « infractions cyber » puisqu'il a vocation à concerner toute infraction pénale pour laquelle les preuves se présentent sous une forme numérique.

Il devrait être ouvert à la signature courant printemps 2022. À suivre.

### 3. Digital Service Act, un vote du Parlement Européen

Le Parlement Européen a voté, le 20 janvier dernier, la proposition de loi sur les services numériques (également connu sous le nom de Digital Service Act). Ce texte doit permettre de « *mieux réguler les géants du numérique* » lesquels devront notamment modérer les contenus en ligne jugés illégaux en Europe et contrôler davantage les biens et services vendus sur leurs plateformes.

Pour rappel, un autre projet de loi, le Data Governance Act, qui a lui vocation à « *réguler la gouvernance des données* » au sein de l'Union Européenne, devrait également voir le jour prochainement. Le Parlement et le Conseil de l'Union Européenne se sont, en effet, accordés sur les conditions de sa mise en œuvre.

### 4. Plateforme d'identification des cybercriminels

La police et la gendarmerie françaises se sont dotées d'une plateforme « *Malware Information Sharing Platform* » destinée à faciliter leurs investigations dans le cadre de cyberattaques.

La mise en œuvre de ce traitement automatisé de données a été autorisé, par [Arrêté du 22 décembre 2021](#).

Il a vocation à centraliser les informations issues des procédures judiciaires ouvertes pour atteintes aux systèmes de traitement automatisé des données. L'objectif recherché est de « *faciliter l'identification de l'auteur* », ainsi que « *les investigations correspondantes par le recoupement et l'analyse de ces informations* ». Les informations contenues dans ce traitement proviennent des logiciels de rédaction des procédures judiciaires de la police nationale et de la gendarmerie nationale, mais également des informations recueillies par le centre d'alerte et de réaction aux attaques informatiques de la police judiciaire. Il est prévu qu'il puisse par ailleurs être alimenté de sources dites ouvertes.

Par délibération en date du 24 juin 2021, la CNIL a formulé un [avis favorable](#) à la mise en œuvre de ce traitement.

#### **5. Régulateur des Marchés Financiers Américains : Sanction de JP MORGAN SECURITIES pour une utilisation de WhatsApp**

Le Régulateur des Marchés Financiers Américains (en anglais, Security Exchange Commission) a sanctionné, JP MORGAN Securities, d'une amende de 200 millions de dollars, en raison d'une utilisation abusive et insuffisamment protégée, en milieu bancaire, de WhatsApp et de SMS.

Elle reproche notamment à la filiale de courtage de JP MORGAN d'être dans l'incapacité de tracer les échanges entre ses collaborateurs (sur leurs équipements personnels) et les clients, de la banque et ce, en violation de la Loi fédérale sur les valeurs mobilières.

Cette loi exige en effet que les sociétés financières conservent des enregistrements méticuleux des messages électroniques survenant entre les courtiers et les clients afin que les régulateurs puissent s'assurer que ces sociétés n'enfreignent pas les lois anti-fraude ou antitrust.

Le Régulateur a annoncé avoir étendu son enquête afin de mettre fin à ces mauvaises pratiques de communication dans le monde de la finance.

#### **6. Enquêtes et sanctions prononcées par les autorités de protection des données personnelles européennes**

##### ➤ **France**

##### **- Sanctions prononcées en 2021 par la CNIL**

La CNIL a prononcé, en 2021, des sanctions avoisinant un montant total de 214 millions d'euros.

Elle a notamment sanctionné des manquements relatifs à la limitation des durées de conservation des données (durées excessives de conservation), au défaut d'information des personnes concernées.

Des sanctions non-pécuniaires ont également été prononcées par la CNIL. Pour rappel, le Ministère de l'Intérieur a écopé d'un rappel à la loi s'agissant de l'utilisation illicite de drones équipés de caméras pour surveiller le respect des mesures de confinement.

Le recours à un système de reconnaissance faciale pour l'identification automatique des personnes faisant l'objet d'une interdiction de stade a également été sanctionné.

Enfin, de nombreuses mises en demeure ont été adressées concernant l'utilisation de cookies tiers.

##### **- Non-respect des droits des personnes concernées et des règles de sécurité**

FREE MOBILE a écopé d'une amende de 300.000 euros pour non-respect des droits des personnes concernées et des règles de sécurité des données.

Cette sanction fait suite à des plaintes reçues, entre décembre 2018 et novembre 2019, de la part d'utilisateurs reprochant à l'opérateur de ne pas prendre en compte leurs demandes d'accès et d'opposition à recevoir des messages de prospection commerciale.

La CNIL a également constaté un manquement à l'obligation de protéger les données, dès la conception et à la sécurité des données. Pour plus d'informations : [cliquer ici](#)

- ***Manquement à la protection des données des utilisateurs***

L'établissement de paiement agréé SLIMPAY a dû s'acquitter d'une amende de 180.000 euros pour insuffisance de protection des données personnelles des utilisateurs et absence d'information d'une violation de données.

En effet, des données concernant environ 12 millions d'utilisateurs (données d'état civil, adresses postales et électroniques, numéros de téléphone et informations bancaires) sont restées stockées, entre juillet 2016 et février 2020, sur un serveur ne faisant l'objet d'aucune sécurité particulière et qui plus est librement accessible sur internet.

La CNIL a par ailleurs constaté un manquement à l'obligation d'encadrer, par un acte juridique, les traitements effectués par un sous-traitant (absence de clauses permettant de s'assurer que les sous-traitants s'engageaient à traiter des données en conformité avec le RGPD).

- ***Cookies***

➤ ***Sanction à l'encontre de FACEBOOK IRELAND LIMITED***

Une amende de 60 millions d'euros (assortie d'une astreinte de 100 000 par jour de retard) a été prononcée, à l'encontre de Facebook Ireland Limited, en raison de l'impossibilité, pour les internautes, de refuser les cookies aussi facilement que de les accepter sur le site [www.facebook.com](http://www.facebook.com).

Au cours d'un contrôle en ligne, faisant suite à la réception de nombreuses plaintes, la CNIL a constaté la présence d'un bouton permettant d'accepter immédiatement les cookies, sans qu'il n'y ait de solution équivalente pour permettre à l'internaute de refuser, aussi facilement, le dépôt.

Au contraire, il a été constaté que plusieurs clics étaient nécessaires pour refuser tous les cookies, contre un seul pour les accepter et que le bouton permettant de les refuser se situait en bas de la seconde fenêtre et s'intitulait « Accepter les cookies ».

La CNIL a considéré que ce mécanisme « *de refus plus complexe revient, en réalité, à décourager les utilisateurs de refuser les cookies et à les inciter à privilégier la facilité du bouton de consentement aux cookies figurant dans la première fenêtre* » et « *qu'un tel procédé portait atteinte à la liberté du consentement des internautes* ».

De même, « *le parcours informationnel mis en œuvre par la société n'est pas clair puisque, pour refuser le dépôt de cookies, les internautes doivent cliquer sur un bouton intitulé « Accepter les cookies » figurant dans la seconde fenêtre* ». Or, « *un tel intitulé génère nécessairement de la confusion* », l'utilisateur pouvant « *avoir le sentiment qu'il n'est pas possible de refuser le dépôt de cookies et qu'il ne dispose pas de modalités de contrôle à cet égard* ».

3 mois ont été octroyés à Facebook pour mettre à la disposition des internautes un moyen permettant de refuser les cookies aussi simplement que celui existant pour les accepter.

- ***Sanction de 150 millions d'euros à l'égard de Google LLC et Google Ireland Ltd***

Le 31 décembre dernier, une amende de 150 millions a été prononcée, pour les mêmes raisons (dépôt de traceurs sans consentement préalable de l'internaute, défaut d'information suffisamment claire sur la finalité des cookies et absence de procédure pour retirer son consentement), à l'encontre de Google LLC (90 millions) et de Google Ireland Limited (60 millions).

Cette sanction, assortie d'une astreinte de 100 000 euros par jour de retard à l'issue d'un délai de trois mois pour se mettre en conformité, fait suite à des plaintes dénonçant les modalités de refus de dépôt de cookies sur [google.fr](http://google.fr) et [youtube.com](http://youtube.com).

Un recours a été initié par Google devant le Conseil d'Etat. L'entreprise considère que la CNIL n'était pas compétente le sanctionner et que cette compétence reviendrait à l'autorité irlandaise au regard de la procédure du [guichet unique](#).

De son côté, la CNIL se considère comme compétente pour sanctionner les infractions en lien avec les traceurs sur la base de la directive e-privacy (les faits relevant matériellement de la directive et non du règlement).

En effet, le considérant 173 du RGPD prévoit que ce règlement n'est pas applicable aux traitements soumis à la directive e-privacy.

Pour rappel par décision ([n° 449212](#)) en date du 4 mars 2021, le Conseil d'Etat français a déjà conclu en l'inapplicabilité du mécanisme du guichet unique en matière de cookies, [cette position ayant été confirmée le 28 janvier 2022](#).

Affaire à suivre pour cette nouvelle amende.

### ➤ **Autriche**

L'autorité de protection des données a récemment jugé que l'utilisation des cookies Google Analytics est illégale. Cette décision s'inscrit dans le prolongement de l'arrêt SCHREMS II rendu par la Cour de Justice de l'Union Européenne. Pour rappel, cet arrêt avait conduit à l'invalidation du Privacy Shield, sur la base duquel les transferts de données vers les Etats-Unis étaient opérés depuis l'Union Européenne.

A la suite de cet arrêt, l'association Noyb (à l'origine des arrêts SCHREMS 1 et 2) avait déposé une centaine de plaintes à l'encontre de sociétés utilisant les cookies Google Analytics pour transfert illégal de données vers les Etats-Unis.

### ➤ **Italie**

#### - ***Appels téléphoniques non désirés***

L'Autorité de protection des données italienne a sanctionné la société ENEL ENERGIA d'une amende de 26,5 millions d'euros en raison de la réception d'appels promotionnels non-désirés y compris des appels pré-enregistrés.

Cette sanction fait suite à des centaines de plaintes adressées à l'Autorité italienne. Au cours des vérifications effectuées au sein de la société mais également de certains de ses partenaires d'affaires, elle a ainsi pu relever qu'ENEL ENERGIA a ciblé, de manière spécifique, des personnes non répertoriées dans l'annuaire téléphonique ou ayant retiré leur consentement pour la réception d'appels promotionnels.

La société n'aurait pas répondu, dans les délais requis, aux demandes d'accès adressées par les personnes concernées et n'aurait pas coopéré suffisamment avec l'autorité de contrôle en violation des articles 30 (registre des activités de traitement) et 31 (coopération avec l'autorité de contrôle) du RGPD.

Parmi les arguments présentés en défense, la société a indiqué que les numéros utilisés pour effectuer les appels téléphoniques ne lui appartenaient pas et n'appartenaient pas à ses partenaires d'affaires.

A cet égard, l'autorité de protection des données a considéré qu'ENEL ENERGIA n'avait pris aucune mesure concernant les appels promotionnels effectués en son nom alors qu'elle avait reçu des plaintes de personnes démarchées en raison de pratiques de télémarketing agressives entraînant ainsi une violation du principe de Privacy By Design. Elle a également retenu qu'ENEL n'a pas été en mesure de prouver le respect des lois sur la protection des

données s'agissant des appels promotionnels non-sollicités réalisés par un de ses partenaires commerciaux et n'a par ailleurs pas contrôlé les activités de ses partenaires.

Il lui a été par ailleurs reproché d'avoir violé le principe d' « accuracy » en associant de manière erronée les données de différentes personnes dans ses registres.

Enfin, concernant son site internet et son application mobile, l'Autorité a relevé la violation des principes de licéité, de loyauté et de transparence.

***Commission de Contrôle des Informations Nominatives***  
***Ce document est à vocation purement informative et ne peut être considéré comme reflétant une position officielle de la CCIN***