Que nous réserve la cybercriminalité dans les 12 prochains mois ?

	Que nous réserve la cybercriminalité dans les 12 prochains mois ?

Depuis ces dernières années, la cybercriminalité fait couler beaucoup d'encre ! Qui n'a pas été touché ou ne connaît pas un proche concerné par un e-mail douteux voire d'arnaque, un site Internet piégé, un programme aux intentions essentiellement malveillantes, un profil menteur-voleur ou même un petit prélèvement à l'étranger ?

Le développement de l'Internet et son nombre d'utilisateurs grandissant a aussi fait grimper le nombre de cyberdélinquants. Si quelques pirates informatiques peuvent être considérés comme de véritables génies, les plus nombreux trouvent sur Internet suffisamment d'informations techniques pour se comporter comme de simples émules et s'en mettre eux aussi plein les poches.
Parce qu'un homme averti en vaut deux, venez découvrir au cours de notre conférence d'1h30, ce que la cybercriminalité va nous réserver dans les 12 prochains mois afin d'y être mentalement et techniquement préparé.

Objectif de la conférence

Améliorez votre confiance et adaptez votre stratégie digitale en tenant compte des tendances des prochaines années en matière de cybercriminalité.

Programme

• Etat des lieux en France et dans le monde;
• Les prochaines techniques utilisées par les pirates;
• Faisons évoluer nos bonnes pratiques ;

Durée

1h30 + 30min à 1h de questions / réponses.

Public concerné :

Clubs d'entreprises, chambres, fédérations, corporations, décideurs, dirigeants, élus, présidents d'associations.

Moyens techniques :

Vidéo projecteur et sonorisation souhaitée selon la taille de la salle.

Animateur :

Denis JACOPINI
Expert Judiciaire en Informatique
Diplômé en cybercriminalité, sécurité de l'information
Droit de l'expertise judiciaire
Risk Manager ISO 27005
Spécialisé en protection des données personnelles
Correspondant CNIL
Gérant d'une SSII pendant 17 ans

Intéressé pour organiser cette conférence ? Contactez-nous

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Combien valent vraiment vos

données personnelles sur les réseaux sociaux ?

	Combien valent vraiment vos données personnelles sur les réseaux sociaux ?

Une extension pour navigateur développée par des chercheurs de l'université de Madrid vous permet de connaître en temps réel les revenus publicitaires générés par votre profil Facebook.

Sur Internet, comme le dit l'adage : si c'est gratuit, c'est vous le produit.
SUPERSTOCK/SUPERSTOCK/SIPA

MONÉTISATION. Dans le monde des *big data*, combien valent vraiment vos données personnelles sur Facebook ? Les recettes publicitaires du réseau social ne cessent de croître de façon exponentielle : 17 milliards de dollars pour 2015, contre 764 millions en 2009. Et combien d'euros gagnés grâce à votre propre activité ? Pour l'usager, il est souvent délicat de répondre à cette question, tant l'opacité sur les algorithmes utilisés par les plate-formes (dont réseaux sociaux) est grande. Mais une extension gratuite pour le navigateur Chrome (bientôt disponible aussi pour Opera et Firefox) développée par des chercheurs de l'Université de Madrid permet d'estimer en temps réel la valeur économique dégagée par votre profil au fur et à mesure du temps passé sur le site de Mark Zuckerberg… un travail de recherche qui interroge d'ailleurs la valeur commerciale globale de nos données et les modes de régulation possibles.

Même sans cliquer sur les pubs, un internaute rapporte

L'outil madrilène, baptisé FDVT (pour *Facebook Data Visualisation Tools*), permet de quantifier l'évolution de la valeur publicitaire d'un profil en fonction du temps passé sur le réseau social. Il s'appuie sur le projet TYPES, financé par l'Europe dans le cadre de l'initiative Horizon 2020, qui se préoccupe de la transparence de la publicité en ligne dans l'économie numérique. *« Chacun a une valeur différente sur le marché selon son profil, de sorte que l'outil ne fournit qu'une estimation des profits »*, expliquent Ángel et Rubén Cuevas, professeurs à l'Université Charles III de Madrid et créateurs de l'extension. *« Lorsque vous vous connectez à Facebook et recevez une publicité, nous déterminons la valeur qui lui est associée, le prix que ces annonceurs paient pour afficher ces publicités et chacun de vos clics sur une de ces publicités. »* Les deux chercheurs ont notamment constaté que le coût d'un utilisateur américain est à peu près deux fois supérieur à celui d'un utilisateur espagnol. Et ce n'est pas tout : ils ont également mis en évidence que même sans jamais cliquer sur un lien sponsorisé, Facebook générait néanmoins de la valeur à partir de votre profil.

Capture d'écran de l'extension : après quelques minutes seulement d'activité et sans cliquer sur aucune pub, l'auteur de ces lignes a déjà cédé près d'un dollar de revenu publicitaire à Facebook.

Une commodité marchande comme les autres ?

À l'heure où les données personnelles s'échangent pour une poignée de dollars (et notamment en Chine, on l'on peut acquérir les données personnelles de citoyens américains pour à peine 100 dollars), se pose la question de leur valorisation. Un rapport écrit fin 2016 par le Oxford Internet Institute s'interrogeait ainsi sur la chaîne de valeur des données personnelles (c'est à dire, l'évolution de leur valeur de leur création à leur utilisation dans l'économie numérique), et sur les types de régulation possibles, par exemple via une possible taxation de l'usage des données personnelles. Une démarche qui n'aurait rien d'évident, au vu de la nature internationale et dématérialisée des échanges de données…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Sur les réseaux sociaux, combien valent vraiment vos données personnelles ? – Sciencesetavenir.fr

---

La Cnil sanctionne « Attractive World » et « Meetic »

La Cnil sanctionne « Attractive World » et « Meetic »

Meetic a indiqué qu'en s'inscrivant sur son site de rencontre, « les personnes ont conscience et sont informées que les données qu'elles fournissent sont nécessaires pour la fourniture du service auxquelles elles souscrivent « , une forme de consentement express en quelque sorte.

Après plusieurs mises en garde, réunions et rencontres avec la CNIL, les deux géants Meetic et Attractive World n'avaient pas fait mine de s'intéresser aux recommandations de l'autorité pour changer un aspect important relatif à la protection des données personnelles. La Commission nationale de l'informatique et des libertés a prononcé, fin décembre 2016, une sanction publique de 10 000 euros à l'encontre de la société Samadhi, propriétaire du site Attractive World et de 20 000 euros à l'encontre de Meetic SAS, en raison du traitement des données *sensibles* de leurs utilisateurs sans recueil de leur consentement exprès.

Il faut dire que ces sites sont de plus en plus thématisés, ciblés, en fonction de goûts ou de communautés. Un point que ne partage pas la CNIL qui déplore un manquement évident à la loi « *Informatique et Libertés* « .

Conséquence, en juillet dernier, 8 sites, et pas des moindres, ont été mis en demeure de rectifier le tir. Visiblement, deux d'entre eux n'ont pas joué le jeu. En effet, en cas d'attaque malveillante à l'encontre de ces sites, donc de piratage informatique, les données personnelles et *sensibles* peuvent se retrouver dans la nature ce qui pourrait être déplorable pour les utilisateurs qui n'ont pas donné leur consentement éclairé sur l'exploitation de leurs données privées, qui plus est, sur leurs affinités, leurs croyances, leurs avis politiques ou leurs origines ethniques.

« Les utilisateurs souhaitant s'inscrire aux sites devaient – en une seule fois – accepter les conditions générales d'utilisation, attester de leur majorité et consentir au traitement des données *sensibles*« , rappelle la Cnil. « La seule inscription au **site de rencontre** ne peut valoir accord exprès des personnes au traitement de telles données qui révèlent **des éléments de leur intimité**« .

Original de l'article : « Attractive World » et « Meetic » épinglés par la Cnil

---

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : « Attractive World » et « Meetic » épinglés par la Cnil

Sécurité des vote électronique en France, comme aux USA ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Sécurité des vote électronique en France, comme aux USA ?				

L'année 2017 sera une grosse année de scrutins, avec l'élection présidentielle en avril-mai et les législatives en juin. Et comme depuis une dizaine d'années qu'un ministre de l'Intérieur, Nicolas Sarkozy, a poussé l'introduction d'ordinateurs de vote en France, des communes vont encore obliger leurs électeurs à voter sur ces machines dont ils ne peuvent contrôler eux-mêmes l'intégrité (en 2012, une soixantaine de communes pour 1,5 million d'électeurs).

Photo: machine à voter utilisée à Stains (Seine-Saint-Denis) aux élections départementales le 22 mars 2015. Chris93/Wikimedia Commons/CC by-sa

Un député socialiste, Sébastien Pietrasanta, vient à cette occasion de poser au gouvernement une question écrite sur « la sécurisation du vote électronique ». Il demande notamment:

« Au-delà d'un risque connu sur la fiabilité des machines et sur la difficulté de recompter les voix, la menace de piratage informatique par des puissances étrangères est hélas d'actualité. Si la menace concerne principalement les partis politiques, à l'instar du piratage des ordinateurs du Parti démocrate aux États-Unis, la possibilité d'une attaque des machines à voter n'est plus à exclure. Aussi, il souhaiterait savoir ce que le ministère de l'intérieur, en charge des élections, compte mettre en place pour assurer la sécurisation du vote lors des élections présidentielle et législatives 2017 et s'il envisage de recourir à un moratoire sur l'utilisation de ces machines électroniques au nom d'un principe de précaution. »

Une position oubliée du PS en 2007

Cette question a été repérée par Nextinpact – qui ironise sur le moratoire « pourtant en vigueur depuis quasiment dix ans », mais il ne s'agit que d'un moratoire sur l'installation du vote électronique dans de nouvelles communes, pas sur son usage dans les villes où il est déjà en place, si c'est dans ce sens que l'entend le député.

Le Parti socialiste, qui en 2007 (quand François Hollande en était premier secrétaire) demandait la suspension du vote électronique, l'a maintenu contre vents et marées depuis son retour au pouvoir en 2012, et indiqué en 2014 encore sa position: ni extension ni abandon (une commune peut choisir de revenir au vote papier, mais au niveau national rien n'est imposé). Donc en 2017, ce sera, encore, circulez il n'y a rien à voir.

La question du député (publiée le 27 décembre) fait référence au piratage du parti démocrate aux Etats-Unis, en pleine actualité puisque c'est une des raisons de l'expulsion de 35 diplomates russes que vient de décider Barack Obama.

L'opacité du vote électronique en soi est aussi un problème crucial: avant l'élection de novembre aux Etats-Unis, un informaticien spécialiste de la sécurité, Bruce Schneier, mettait en garde contre les risques de piratage des machines de vote électronique.

USA: toutes les machines peuvent être piratées

Un reportage de Pixels/Le Monde, depuis le Chaos Computer Congress cite deux chercheurs de l'université du Michigan, Alex Halderman et Matt Bernhard, qui ont participé aux recomptages de certains Etats après le scrutin. S'ils pensent, sans en être certains, que le vote de novembre n'a pas été piraté, ils pointent les nombreuses vulnérabilités du système de vote américain:

« Première faiblesse : les machines à voter. Plus de 50 modèles différents existent et, selon les chercheurs, toutes peuvent être piratées. 'De nombreuses machines à voter ont été étudiées, par des chercheurs indépendants, et dans tous les cas, il a été prouvé que la machine était vulnérable à l'injection de programmes informatiques malveillants faussant les résultats', explique M. Halderman.

Les responsables des élections objectent que ces machines ne sont pas connectées à Internet et sont donc protégées. Cela ne fait aucune différence, explique M. Bernhard, puisque est insérée dans chaque machine, et avant chaque scrutin, une carte mémoire contenant les paramètres du vote. C'est aussi dans cette carte que sont stockés les résultats. Or, les ordinateurs qui paramètrent ces cartes sont fréquemment connectés à Internet. »

Autre faiblesse, l'absence de contrôle a posteriori: plus de 70% des votes aux Etats-Unis ont une trace en papier. « Il faudrait comparer les votes contenus dans les cartes mémoires et la trace en papier, mais malheureusement la plupart des Etats ne le font pas. » Un peu comme en France: le meilleur moyen de prétendre que le vote électronique a bien marché, c'est de ne surtout pas vérifier après coup…[lire la suite]

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Délibération n° 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique

Vous avez un doute sur la sécurité de vos machines à voter ?
Vous souhaitez un expert indépendant spécialisé en votes électroniques pour expertiser le système de vote électronique que vous avez choisi ?
Nous pouvons expertiser leur sécurité en rapport avec la délibération de la CNIL n° 2010-371 du 21 octobre 2010.
Contactez-nous

Réagissez à cet article

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?

La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle

Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ?
Cliquez ici pour une demande de chiffrage d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :
• Expert en Informatique **assermenté et indépendant** ;
• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;
• et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Original de l'article mis en page : Vote électronique: en France, aux USA, tout baigne? Hum… – ZDNet

---

Et si je vous remerciais par avance pour vos voeux 2017 ?

Et si je vous remerciais par avance pour vos voeux 2017 ?

Avignon, le 29/12/2016

A force de voir les rayons remplis de cartables avant même la fin de l'année scolaire et des rayons de guirlandes et de sapins vierges dès la fin de l'été, j'ai souhaité garder le rythme et, pour ne pas vous choquer, attendre un peu pour vous souhaiter de joyeuses pâques mais déjà vous remercier pour les vœux 2017 que vous allez dans les 30 prochains jours m'envoyer.

Pour terminer, sans pour autant critiquer ni protester contre les envois en masse de messages tous aussi impersonnels les uns que les autres, je tiens par contre du coup, à vous envoyer ce message personnalisé. La preuve, il n'est que pour vous.

Réagissez à cet article

Le RGPD règlement européen de protection des données et les contrats fournisseurs

	Le RDPD, règlement européen de protection des données et les contrats fournisseurs

Entré en vigueur en mai dernier, le Règlement général sur la protection des données impose de nouvelles règles en matière de gestion des données personnelles. Avec l'obligation pour les entreprises de se mettre en conformité avant mai 2018. Ce qui implique une modification des contrats fournisseurs.

Qui est concerné?

Le RGPD s'applique « au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. »

Ce règlement s'applique à toute structure (responsable de traitement des données ou sous-traitant) ayant un établissement dans l'Union européenne ou bien proposant une offre de biens ou de services visant les personnes qui se trouvent sur le territoire de l'Union européenne.

Les actions de profilage visant cette cible sont également concernées. Ainsi, alors que la loi Informatique et libertés se basait sur des critères d'établissement et de moyens de traitement, le règlement européen 16-679 introduit la notion de ciblage: le critère principal d'application est désormais le traitement des données d'une personne se trouvant au sein de l'UE.

Qu'est-ce qu'une donnée à caractère personnel?

L'une des difficultés posées par le RGPD va consister à définir les données personnelles concernées. Le règlement stipule qu'il s'agit de « toute information concernant une personne physique identifiée ou identifiable », directement ou indirectement.

Des données indirectement identifiantes, telles qu'un numéro de téléphone, ou un identifiant, sont donc concernées. De même, les données comportementales collectées sur Internet (notamment recueillies dans le cadre d'actions marketing de profilage), si elles sont corrélées à une identité, deviennent des données à caractère personnel.

Selon le traitement appliqué aux données, des informations non identifiantes peuvent ainsi devenir identifiantes, par croisement des informations collectées.

Quelles obligations pour les entreprises?

La loi Informatique et libertés se basait sur du déclaratif initial et des contrôles ponctuels. Le nouveau règlement européen remplace cette obligation de déclaration par une obligation de prouver à chaque moment que l'entreprise protège les données. Dès lors, la structuration même des outils permettant la collecte des données (CRM, DMP, solutions de tracking ou de géolocalisation…), mais aussi les contrats passés avec les fournisseurs et clients sont impactés (voir encadré ci-dessous).

« Le règlement couple des notions techniques et juridiques », souligne Thomas Beaugrand, avocat au sein du cabinet Staub & Associés. Il introduit des nouveaux principes et concepts qui renvoient désormais vers plus de précautions techniques. Par ailleurs, les entreprises ont, entre autres, l'obligation de donner la finalité précise de la collecte des données (il s'agit du principe de minimisation, un des grands principes de la dataprotection, qui impose que seules les données nécessaires à la finalité poursuivie pourront être collectées).

Le GRPD impose également le principe de conservation limitée des données, ainsi que celui de coresponsabilité des sous-traitants et des entreprises en matière de protection de la data, qui permet de distribuer les responsabilité en fonction de la mainmise de chacun sur les données. Cette notion de coresponsabilité doit être intégrée dès maintenant dans les contrats passés avec les fournisseurs: en effet, le sous-traitant désigné par une organisation pour assurer le traitement des données devient, avec le RGPD, coresponsable de la légalité des traitements. Il sera donc tenu d'informer ses clients et de tenir des registres pour recenser les données, ainsi que d'accepter les audits demandés par son client pour s'assurer de la conformité des traitements.

Les sous-traitants concernés peuvent être, par exemple, l'éditeur d'un CRM en ligne, le routeur d'une campagne d'e-mailing, un service de relation client, etc. Le responsable du traitement, de son côté, doit s'assurer que ses fournisseurs ont pris les mesures nécessaires pour assurer la sécurité des données.

Enfin, parmi les changements majeurs, la nomination d'un DPO, ou délégué à la protection des données, qui sera obligatoire dans tout le secteur public, ainsi que dans les structures privées qui font des traitements de données exigeant un suivi régulier et systématique des personnes à grande échelle (dans le secteur du marketing, notamment). Il sera le garant de la conformité au règlement. Quel impact sur les contrats fournisseurs? Pour se mettre en conformité avec le RGPD, les directeurs achats devront veiller à renforcer les contrats passés avec leur fournisseurs…[lire la suite]

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Le règlement européen de protection des données et les contrats fournisseurs

Le règlement européen de protection des données et les contrats fournisseurs

Le règlement européen de protection des données et les contrats fournisseurs

Le Règlement général sur la protection des données (RGPD) du 27 avril 2016 est paru au JO le 4 mai 2016.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la protection des données Personnelles et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif à la Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur notre page formations.

Réagissez à cet article

Vote électronique aux élections professionnelles

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Vote électronique aux élections professionnelles				

Le Décret n° 2016-1676 du 5 décembre 2016 relatif au vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise est publié.

Désormais, le chef d'une entreprise employant au moins 11 salariés peut recourir au vote électronique pour ses élections professionnelles et ce même en l'absence d'un accord collectif.
Il peut dorénavant décider de fixer lui-même les modalités du vote électronique, sous réserve de respecter les conditions fixées par le décret du 5 décembre 2016.
L'employeur d'au moins 11 salarié peut ainsi décider de recourir au vote électronique pour les élections partielles se déroulant en cours de mandat.
Il choisit, dans ce cas, si le vote électronique interdit ou pas le vote à bulletin secret sous enveloppe.
Le chef d'une entreprise employant au moins 11 salariés doit établir un cahier des charges respectant les dispositions réglementaires relatives au vote électronique et le tenir à la disposition des salariés sur le lieu de travail et sur l'intranet de l'entreprise.
Attention : pendant le déroulement du scrutin, aucun résultat partiel n'est accessible.
Seul, le nombre de votants peut, si l'employeur le prévoit, être révélé au cours du scrutin.
Par **Carole Vercheyre-Grard**
Avocat au Barreau de Paris
Source juritravail.com

Réagissez à cet article

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?

La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle

Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ? Cliquez ici pour une demande de chiffrage d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :
• Expert en Informatique **assermenté et indépendant** ;
• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;
• et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.
Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.
Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.
Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Original de l’article mis en page : Vote électronique aux élections professionnelles

---

Le Règlement Général sur la Protection des Données (RGPD) en détail

Le Règlement Général sur la Protection des Données (RGPD) en détail

---

Après quatre années d'âpres négociations, les États Membres de l'Union Européenne sont enfin convenus d'un texte venant moderniser la directive 1995/46/CE du 24 octobre 1995, laquelle datait des débuts d'Internet. Mais, contrairement à une directive, le Règlement adopté le 8 avril 2016 par le Conseil de l'Europe puis, le 16 avril, par le Parlement européen, est d'application directe et s'imposera aux États Membres à compter du 25 mai 2018, sans qu'il soit besoin de le transposer dans les législations nationales.

Le processus d'élaboration du texte, long et émaillé de près de 4000 amendements, a mis au monde un texte très long – plus de 200 pages – comportant 99 articles introduits par 173 considérants.
Intitulé *« Règlement n°2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données »*, le texte résultant, complexe et technique, est particulièrement difficile à aborder par les entreprises et les administrations, lesquelles sont pourtant les principaux acteurs visés par le texte. Ainsi, dans un article du 18 octobre 2016, le journal La Tribune écrivait que *« 96% des entreprises des trois principales économies européennes [France, Allemagne, Royaume-Uni] ne comprennent pas encore clairement le Règlement général de protection des données (RGPD) (…) Selon une étude publiée ce mardi par la société de sécurité informatique Symantec, 92% des dirigeants et décideurs français s'inquiètent de ne pas être en conformité au moment de l'entrée en vigueur de la RGPD »* !
Les acteurs du traitement de données vont donc devoir investir considérablement pour se mettre à niveau de la nouvelle réglementation, d'autant que toutes les entreprises du monde traitant des données personnelles de citoyens européens sont concernées par le Règlement.
Nous nous proposons, à travers cet article, d'exposer les principales nouveautés du texte sous une forme compréhensible pour le non-initié. Nous dresserons au préalable un tableau général des intentions du texte (I) avant d'insister sur ses innovations principales (II).

I- Présentation générale du RGPD
Le but déclaré du texte est de renforcer le contrôle des citoyens européens sur l'utilisation de leurs données personnelles, tout en simplifiant, en l'unifiant, la réglementation pour les entreprises.
Les citoyens pourront désormais réclamer contre l'utilisation abusive de leurs données auprès d'une autorité unique, chargée de la protection des données, plutôt que de devoir le faire auprès de l'entreprise détentrice de leurs données. Les particuliers pourront également se joindre à des recours collectifs via des organisations représentatives qui, si la loi nationale les y autorise, pourront agir de leur propre initiative.
Le RGPD développe ainsi considérablement les droits reconnus à la personne dont les données sont collectées. Ainsi, des trois droits reconnus à la personne par la loi Informatique et Liberté (opposition au traitement sous réserve de motif légitime, droit d'accès/communication aux données, droit de rectification/suppression), l'on passe à 11 droits (droit à une information complète en langage clair, droit à l'oubli, droit à la limitation du traitement, droit à la portabilité des données, droit d'opposition (notamment au profilage), etc …). D'une manière générale, la personne concernée dispose d'un droit étendu et facilité à accéder aux données à caractère personnel qui la concernent et le texte réaffirme les principes essentiels de la protection de la vie privée :
• Restriction d'utilisation ;
• Minimisation des données ;
• Précision ;
• Limitation du stockage ;
• Intégrité ;
• Confidentialité.
Les entreprises sont incitées à privilégier l'utilisation de pseudonymes avant et pendant le traitement des données pour en garantir la protection (concept de la prise en compte du respect de la vie privée dès la conception). La *« pseudonymisation »* consiste à s'assurer que les données sont conservées sous une forme ne permettant pas l'identification directe d'un individu sans l'aide d'informations supplémentaires.

II- Principales mesures du RGPD

1. Réalisation d'une analyse d'impact avant la mise en place d'un traitement de données
Avant la mise en place d'un traitement de données pouvant présenter des risques pour la protection des données personnelles, l'entreprise devra réaliser une analyse d'impact : *« Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. »* (Article 35 du Règlement)
Le RGPD introduit ainsi le concept de prise en compte du respect de la vie privée dès la conception du traitement : les différentes obligations pesant sur la collecte des données doivent être prises en compte dès la conception du traitement de données (*« privacy by design and by default »*).

2. Consentement clair et explicite à la collecte des données
La directive 1995/46/CE donnait une définition du consentement à la collecte des données, laquelle a été transposé de manière très hétérogène dans les législations nationales, certaines exigeant un consentement explicite, d'autres décidant qu'un consentement implicite était suffisant. Notre loi Informatique et Liberté se contente ainsi de définir des cas dans lesquels le consentement devrait être explicite. Le Règlement vient unifier une fois pour toute cette définition au onzième point de son article 4 consacré aux définitions, en définissant le consentement comme *« toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement »*.
Ce consentement doit donc être express. Il doit résulter d'un acte positif. La personne doit réellement avoir été mise devant la nécessité de donner son accord au traitement. Ainsi, dans son considérant n°32, le Règlement précise qu' *« il ne saurait dès lors y avoir de consentement en cas de silence, de case cochée par défaut ou d'inactivité. »* Plus encore, la charge de la preuve du consentement pèse sur le responsable du traitement (article 7, 1°). En outre, la personne dont les données sont collectées peut retirer son consentement à tout moment (article 7, 3°).
Malgré cela, le Règlement prévoit un certain nombre de cas pour lesquels le traitement demeure licite même sans consentement (article 6, b) à f)) :
• Lorsque ce traitement est nécessaire à l'exécution d'un contrat accepté par la personne ;
• Lorsque le traitement découle d'une obligation légale ;
• Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne ;
• Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ;
• Tout autre intérêt légitime du responsable du traitement, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne, en particulier s'il s'agit d'un enfant.

3. Accès facilité de la personne à ses données
Les personnes dont les données sont collectées disposent de droits à la rectification, à l'effacement des données et à l'oubli : *« la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données la concernant et le responsable du traitement a l'obligation d'effacer ces données dans les meilleurs délais »* (Article 17), et ce pour six motifs : les données ne sont plus nécessaires, la personne concernée retire son consentement, la personne concernée s'oppose au traitement à des fins de prospection, les données ont fait l'objet d'un traitement illicite, les données doivent être effacées pour respecter une obligation légale, ou encore les données ont été collectées dans le cadre d'une offre de service à destinations de mineurs.

4. Notification des violations de données personnelles (« Data Breach Notification »)
A l'heure actuelle, les différentes directives européennes font peser sur les entreprises du secteur de la télécommunication l'obligation d'informer les autorités en cas *« d'accès non autorisé »* à des données personnelles. En clair, lors d'un piratage. Le Règlement, quant à lui, généralise cette obligation de signalement à l'ensemble des responsables de traitement, en ce compris leurs sous-traitants, et ce au plus tard 72 heures après la découverte du problème (Article 33). Bien entendu, il faut que le problème atteigne une certaine gravité pour qu'il soit nécessaire de le rapporter, et tout va donc dépendre de la détermination du seuil à partir duquel le signalement devient obligatoire. L'article 34 du Règlementindique que ce signalement devra intervenir *« lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique. »* L'emploi du mot *« élevé »* laisse donc place à appréciation et donnera donc probablement lieu au développement d'une jurisprudence abondante.
Les personnes concernées par la violation des données doivent également être notifiées dans les meilleurs délais, sauf si des mesures de protection ont été mises en œuvre ou seront prises ultérieurement.

5. La création et la maintenance d'un registre des traitements devient obligatoire
Aux termes de l'article 30 du RGPD, un registre détaillé des traitements doit désormais être obligatoirement conservé non seulement par le responsable du traitement mais également par ses éventuels sous-traitants. Ce registre doit pouvoir être mis à tout moment à disposition des autorités de contrôle.
Le texte insiste ainsi sur la responsabilité du contrôleur des données, lequel est responsable de la conformité du traitement avec le Règlement et doit être, à tout moment, en mesure de la démontrer.
Lorsque le traitement de données est délégué par le responsable du traitement à un sous-traitant, ou *« data processor »*, même situé hors de l'Union Européenne, celui-ci a désormais les mêmes obligations que le responsable du traitement, y compris la désignation d'un délégué à la protection des données, et ce même dans le cas d'un traitement de données gratuit.

6. Création des délégués à la protection des données (Data Protection Officer)
Si notre loi Informatique et Liberté, et ses mises à jour, ont créé le Correspondant Informatique et Liberté (le *« CIL »*), le Règlement, quant à lui, rend obligatoire dans certains cas la nomination d'un délégué à la protection des données (DPD ou, en anglais, DPO : Data Protection Officer) pour les organismes privés ou publics dont *« les activités de base (…) exigent un suivi régulier et systématique à grande échelle des personnes concernées »* ou lorsque *« le traitement est effectué par une autorité publique ou un organisme public »* (article 37), à l'exception des juridictions. Ce délégué n'est obligatoire que dans certains cas, mais il est fortement recommandé de le nommer systématiquement puisque toute entreprise ou administration doit être capable à tout moment de rendre comptes à l'autorité de contrôle de l'état de ses traitements de données.
Le rôle du délégué à la protection des données sera de garantir la conformité des traitements de données avec les principes de protection de la sphère privée, tels que fixés par le RGPD, ainsi que de gérer les relations entre les personnes concernées (employés, clients) et les autorités de surveillance.

7. Le transfert des données est soumis à vérification et peut être demandé par la personne elle-même
Les transferts de données personnelles vers des pays étrangers sont désormais soumis à la vérification des garanties offertes par les lois de ce pays pour préserver un niveau de sécurité équivalent pour les données. L'article 45 du Règlement prévoit que, dans l'idéal, le pays destinataire devra être listé par la Commission européenne. A défaut, des clauses de garantie spéciales devront être prévues dans les contrats, outre la possibilité de recourir à des codes de conduite, des certifications et autres labels. Auquel cas, il ne sera pas nécessaire d'obtenir une autorisation auprès de l'autorité nationale du pays d'origine des données.
En outre, l'article 49 du Règlement prévoit que, si le traitement nécessitait de recueillir le consentement de la personne, alors celle-ci devra être informée du transfert de ses données et des risques que présentent l'opération. Ceci, bien entendu, afin de permettre à la personne de revenir éventuellement sur son consentement.
Enfin, les personnes dont les données sont collectées disposent elles-mêmes d'un droit à demander le transfert des données les concernant (ou *« droit à la portabilité des données »*) vers un autre fournisseur de services : *« Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle »* (Article 20).

8. Restriction du profilage automatisé servant de base à une décision
L'article 21 du Règlement dispose que *« La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire »*, sauf si ce traitement est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement, ou bien que la décision est autorisée par le droit de l'Union européenne, ou bien encore que le consentement explicite de la personne concernée a été recueilli en amont.

9. Recours et aggravation considérable des sanctions
La directive 1995/46/CE prévoyait jusqu'ici simplement la possibilité, pour la personne dont les droits ont été violés, de recourir aux tribunaux et d'obtenir du responsable du traitement réparation de son préjudice.
Le Règlement prévoit quant à lui un *« droit à un recours effectif »* (articles 78 et 79) et un *« droit à réparation »* (article 82). Il définit des règles de compétences des juridictions se substituant aux règles de droit international privé des États Membres et détermine les amendes qui devront être délivrées par les autorités nationales de contrôle (article 83). Or, les amendes mises en place par le Règlement sont considérables, puisqu'elles peuvent aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial ! Le risque qui pèse sur les entreprises imprudentes est donc très sérieux…[lire la suite]

Notre métier :
Nous proposons des service d'accompagnement sur plusieurs niveaux :
1/ Au niveau des utilisateurs qui, face à la résistance au changement, doivent comprendre l'intérêt des démarches de mise en conformité des traitements des données personnelles, pour favoriser leur implication et faciliter la mission du Correspondant aux Données Personnelles.
1'/ Au niveau des utilisateurs encore pour sensibiliser les utilisateurs aux différentes formes d'attaques et d'arnaques informatiques (cybercriminalité) dont les établissements sont très largement victimes.
Les services chargés de gérer les fournisseurs sont fortement incités à suivre notamment un module sur les arnaques aux FOVI et à voir leurs procédures auditées et probablement améliorées.
2/ Au niveau de l'établissement complet afin de faire un état des lieux des traitements concernés et un audit des mesures de sécurité en place et à faire évoluer pour les rendre acceptables vis à vis de la Réglementation relative aux Données Personnelles.
3/ Au niveau du futur CIL ou du futur DPO afin de lui faire découvrir ses misions, l'accompagner dans sa prise de fonction et l'accompagner au fil des changements.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : RGPD : le Règlement Général sur la Protection des Données qui bouleverse la loi Informatique et Liberté. Par Bernard Rineau, Avocat, et Julien Marcel, Juriste.

Vigilance – faux appels passés au nom de la CNIL

Vigilance – faux appels passés au nom de la CNIL

Vigilance – faux appels passés au nom de la CNIL

Des entreprises ont reçu, ces derniers jours, des appels téléphoniques de personnes se faisant passer pour la CNIL et prétextant devoir envoyer des documents.
Ces appels frauduleux ont pour but de collecter des informations sur votre organisation, et notamment l'adresse mail de dirigeants (directeur informatique, directeur des achats, etc.), pour préparer une attaque informatique (rançongiciel / ransomware) ou une escroquerie financière (« arnaque au Président »).
N'y répondez pas ! En cas de doute, vous pouvez contacter la CNIL au 01 53 73 22 22

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l’article mis en page : Vigilance – faux appels passés au nom de la CNIL | CNIL