## Comment se comporte notre cerveau surchargé par le numérique



Comment se comporte notre cerveau surchargé par le numérique Samedi 3 septembre, ARTE a diffusé un excellent reportage sur la manière dont notre cerveau se comporte face à nos vies de plus en plus hyper connectées : « HYPERCONNECTÉS : LE CERVEAU EN SURCHARGE ».

Grâce aux smartphones, ordinateurs et autres tablettes, nous sommes reliés au monde en continu. Mais ce déluge d'informations menace notre bien-être. Alliant témoignages de cadres victimes de burn out et explications de chercheurs en neurosciences, en informatique ou en sciences de l'information et de la communication, ce documentaire captivant passe en revue les dangers de cette surcharge sur le cerveau. Il explore aussi des solutions pour s'en prémunir, des méthodes de filtrage de l'information aux innovations censées adapter la technologie à nos besoins et à nos limites.

Chaque jour, cent cinquante milliards d'e-mails sont échangés dans le monde. Les SMS, les fils d'actualité et les réseaux sociaux font également partie intégrante de notre quotidien connecté, tant au bureau qu'à l'extérieur. Nous disposons ainsi de tout un attirail technologique qui permet de rester en contact avec nos amis, nos collègues, et qui sollicite sans cesse notre attention. Comment notre cerveau réagit-il face à cette avalanche permanente de données ? Existe-t-il une limite au-delà de laquelle nous ne parvenons plus à traiter les informations ? Perte de concentration, stress, épuisement mental, voire dépression...: si les outils connectés augmentent la productivité au travail, des études montrent aussi que le trop-plein numérique qui envahit nos existences tend à diminuer les capacités cognitives.

Un documentaire de Laurence Serfaty (France, 52´), diffusé sur ARTE le samedi 3 septembre à 22h20

A voir et à revoir sur Arte +7 pendant encore quelques jours ! si vous ne voyez pas la vidéo, le lien



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés);
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Objets connectés pour la santé : une étude révèle des failles de sécurité inquiétantes



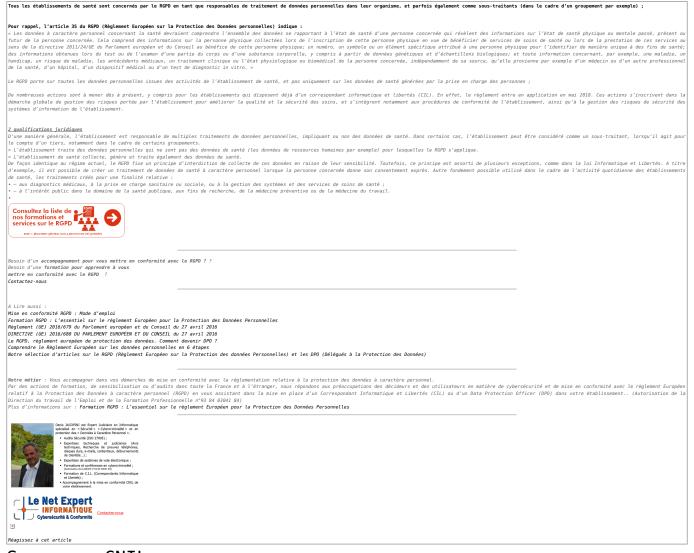
Mashable FR a pu consulter en exclusivité une étude révélant le manque de sécurité de trois objets connectés pour la santé. Des résultats inquiétants lorsqu'on sait qu'un nombre croissant d'utilisateurs font aveuglément confiance à ces outils....[Lire la suite]

```
[block id="24761" title="Pied de page HAUT"]
[block id="24881" title="Pied de page Contenu Cyber"]
[block id="24760" title="Pied de page BAS"]
```

## RGPD : Obligations des pharmacies



RGPD : Obligations des pharmacies



Source : CNIL

Google veut jouer à Madame Irma et anticiper les problèmes de santé avec l'Intelligence Artificielle



Google veut jouer à Madame Irma et anticiper les problèmes de santé avec l'Intelligence Artificielle Prévenir plutôt que guérir : si la grande majorité des médecines traditionnelles de par le monde appliquent déjà ce principe depuis des milliers d'années, il semblerait que la technologie puisse intégrer, elle aussi, ce principe de prévention. Et c'est bien l'intention de Google avec ce nouveau développement de son pôle de recherche scientifique, Google Brain. Cela donnerait un coup de pouce géant à certains domaines de la médecine moderne, notamment en termes de prévision et prévention des maladies cardio-vasculaires, de plus en plus nombreuses, chez les hommes comme chez les femmes.

Google s'est associé avec les universités américaines de Chicago et de San Francisco, afin de concevoir une technologie qui, grâce à l'intelligence artificielle et aux données récupérées par les hôpitaux parmi les milliers de dossiers médicaux des patients, permettrait de pouvoir prédire des risques médicaux, une projection de l'état de santé posthospitalisation, ou les arrêts cardiaques, entre autres espérances…[lire la suite]

**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 d'expertises, d'audits, de formations et de sensibilisation 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



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005);
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés);
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

Source : Intelligence artificielle : Google veut jouer à Madame Irma et anticiper les problèmes de santé

### Les données de santé des Français désormais en libre accès



Dans un communiqué du 10 avril 2017, le gouvernement a indiqué qu'il ouvrait l'accès aux données issues du Système national des données de santé (SNDS) aux organismes exerçant une mission de service public pour toute étude, recherche et évaluation présentant un intérêt public. Ces organismes peuvent désormais consulter et exploiter les données du SNDS suivant certaines conditions détaillées dans le décret du 26 décembre 2016.

### Ainsi, comme le précise le gouvernement :

- L'État, l'Assurance maladie, l'Agence nationale de sécurité du médicament et des produits de santé (ANSM), la Haute Autorité de santé (HAS) ou encore Santé publique France peuvent accéder aux données du SNDS de manière permanente pour leur permettre d'assumer leurs missions
- Les équipes de recherche des centres hospitaliers universitaires (CHU), de l'Institut national de la santé et de la recherche médicale (INSERM) et des centres de lutte contre le cancer peuvent désormais consulter l'échantillon correspondant à 1/100ème de la population.
- Les autres organismes publics ou privés, à but lucratif ou non lucratif, auront eux aussi prochainement accès aux données issues de cette base pour toute étude, recherche et évaluation présentant un intérêt public. Ils seront, eux-aussi, soumis aux conditions précisées dans le décret du 26 décembre 2016

La loi interdit l'usage de ces informations pour deux finalités :

- La promotion commerciale des produits d'assurance santé
- La modulation des contrats d'assurance santé (évolution des primes, exclusions,...

Toutefois, cette annonce suscite des craintes et la réprobation, notamment chez certains acteurs de la santé. Ainsi, la Fédération des Médecins de France — syndicat qui regroupe près de 3000 adhérents — s'oppose à cette mesure. « Si la loi autorise des accès à cette vaste base de données au nom de la recherche et annonce la future possibilité à des entreprises lucratives de pouvoir y accéder également, la FMF rappelle que les données du SNDS ne seront pas anonymisées mais seulement pseudonymisées avec une possibilité d'identification. » explique le syndicat dans un communiqué.

La FMF alerte:

— du risque élevé de perte de confidentialité de leurs données personnelles, soit en raison du piratage, soit en raison du nombre élevé de personnes potentiellement concernées par l'accès aux données du SNDS. La CNIL elle-même a estimé que « le niveau de sécurité envisagé ne sera pas atteint au lancement du traitement SNDS en mars 2017 »[1]. Bien que la loi prévoie un agrément très sévère pour les hébergeurs de données de santé, les mini serveurs de données, de radiologie ou de biologie, permettant un accès rapide aux résultats, ne sont pas tous agréés, et leur accès est très modérément protégé...[lire la suite]

**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 d'expertises, d'audits, de formations et de sensibilisation 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



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005);
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés);
- Accompagnement à la mise en conformité CNIL de



Source : Les données de santé des Français désormais en accès libre —

Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé »



Décret n° 2016-1871 du cembre 2016 relatif au tement de données à caractère de nommé « système l des données données de santé »



Ce texte entre en vigueur le 1er avril 2017. Par application de la loi de modernisation de notre système de santé, il « décrit les modalités de gouvernance et de fonctionnement du système national des données de santé (SNDS) qui a vocation à regrouper les données de santé de l'assurance maladie obligatoire, des établissements de santé, les causes médicales de décès, les données issues des Maisons départementales des personnes handicapées ainsi qu'un échantillon de données de remboursement d'assurance maladie complémentaire ».

« Il fixe en outre la liste des organismes, établissements et services bénéficiant d'accès permanents aux données du SNDS en raison de leurs missions de service public ainsi que les modalités de ces accès. Ce texte prévoit également des possibilités d'accès ponctuel aux données du SNDS. Enfin, il prévoit l'information des personnes auxquelles les données se rapportent, et leurs droits d'accès, de rectification et d'opposition qui s'exercent auprès de la caisse d'assurance maladie dont dépend la personne ».

### Consulter

- Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé »
- Délibération n° 2016-316 du 13 octobre 2016 portant avis sur un projet de décret en Conseil d'Etat relatif au Système national des données de santé (demande d'avis n° 16018114)

**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 d'expertises, d'audits, de formations et de sensibilisation 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

 $: \ https://www.lenetexpert.fr/formations-cybercriminal ite-protection-des-donnees-personnelles\\$ 



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005);
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés);
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

×

Source : Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé » — APHP DAJ

## Les données de santé, la nouvelle cible des cybercriminels



Les données de santé nouvelle cible des cybercriminels Face au développement massif des nouvelles technologies, nos données personnelles sont aujourd'hui entièrement informatisées. De notre dossier médical jusqu'à nos données bancaires en passant par nos loisirs et notre consommation quotidienne, chaque minute de nos vies produit une trace numérique sans même que l'on s'en aperçoit.

Pendant des années nos données de santé étaient éparpillées entre médecins, laboratoire d'analyses, hôpitaux, dentistes dans des dossiers cartonnés qui s'accumulaient au coin d'un bureau ou sur une étagère. En 2012 la loi « hôpital numérique » avait permis un premier virage en obligeant la numérisation des données de santé par tous les professionnels pour une meilleure transmission inter-service. Depuis un an, la loi « santé 2015 » oblige à une unification et une centralisation des données de santé dans des serveurs hautement sécurisés constituant ainsi le Big Data.

### Une centralisation des données qui n'est pas sans risque

Appliqué à la santé, le Big Data ouvre des perspectives réjouissantes dans le croisement et l'analyse de données permettant ainsi d'aboutir à de véritables progrès dans le domaine médical. Mais cela n'est pas sans risque.

Le statut strictement confidentiel et extrêmement protégé donne à ces données une très grande valeur. Nos données médicales deviennent ainsi la cible d'une nouvelle cybercriminalité, cotées sur le Dark Web.

Le Dark Web ou Deep Web est l'underground du net tel qu'on le connait. Il est une partie non référencée dans les moteurs de recherche, difficilement accessible où le cybertrafic y est une pratique généralisée. Sur le Dark Web les données personnelles sont cotées et prennent ou non de la valeur selon leur facilité d'accès et leur rendement.

Là où les données bancaires détournées sont de plus en plus difficiles à utiliser suite aux nombreuses sécurisations mise en place par les banques, l'usurpation d'identité et la récolte de données médicales prennent une valeur de plus en plus grande. Selon Vincent TRELY, président-fondateur de l'APSSIS, Association pour la Sécurité des Systèmes d'information, interviewer sur France Inter le 8 septembre 2016, le dossier médical d'une personne aurait une valeur actuelle qui peut varier entre 12 et 18 \$.

Si l'on rapporte cette valeur unitaire au nombre de dossiers médicaux abrités par un hôpital parisien, on se rend compte que ceux-ci abritent une potentielle fortune pouvant aller jusqu'à des millions de dollars. Aussi pour protéger ces données, les organismes de santé se tournent vers des sociétés certifiées proposant un stockage dans des Datacenters surveillés, doublement sauvegardés, ventilés avec une maintenance 24h/24. Le stockage a donc un coût qui peut varier entre quelques centaines d'euros jusqu'à des centaines de milliers d'euros pour un grand hôpital. Le coût d'hébergement peut alors devenir un vrai frein pour des petites structures médicales où le personnel présent est rarement qualifié pour veiller à la sécurité numérique des données. Et c'est de cette façon que ces organismes deviennent des cibles potentielles pour les cybercriminels.

Des exemples il en existe à la Pelle. Le laboratoire Labio en 2015 s'est vu subtilisé une partie des résultats d'analyse de ses patients, pour ensuite devenir la victime d'un chantage. Les cybercriminels demandaient une rançon de 20 000 euros en échange de la non divulgation des données. Peu de temps après c'est le service de radiologie du centre Marie Curie à Valence qui s'est vu refuser l'accès à son dossier patients bloquant ainsi toute une journée les rendez-vous médicaux initialement fixés. Peu de temps avant, en janvier 2015, la Compagnie d'Assurance Américaine Anthem a reconnu s'être fait pirater. Toutes ses données clients ont été cryptées en l'échange d'une rançon.

Ces pratiques étant nouvelles, on peut s'attendre à une recrudescence de ce type de criminalité dans l'avenir selon les conclusions en décembre 2014 de la revue MIT Tech Review…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons conférences et formations pour sensibiliser décideurs et utilisateurs aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles. Nos actions peuvent être personnalisées et organisées dans votre établissement.

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



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...):
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés);
- Accompagnement à la mise en conformité CNIL de votre établissement.

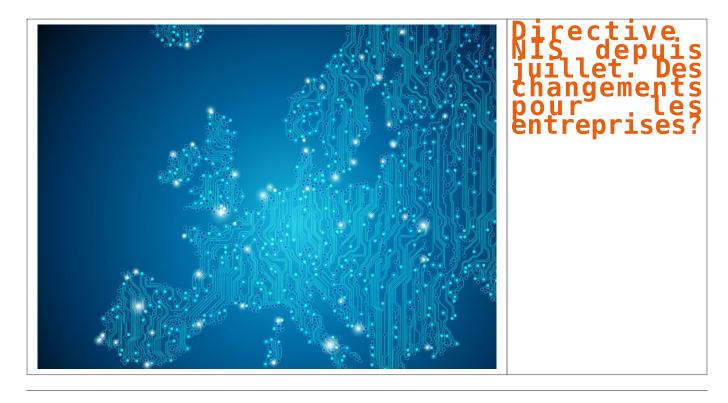


Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Les données de santé, le nouvel El-Dorado de la cybercriminalité

# Directive NIS adoptée: quelles conséquences pour les entreprises?



En juillet dernier, le Parlement européen a adopté la directive NIS (Network and Information Security). Les opérateurs de services ainsi que les places de marché en ligne, les moteurs de recherche et les services Cloud seront soumis à des exigences de sécurité et de notification d'incidents.

C'est fait ! La directive NIS a été approuvée le 6 juillet par le Parlement européen en seconde lecture, après avoir été adoptée en mai dernier par le Conseil de l'Union européenne. Cette directive est destinée à assurer un « niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne ». Les « opérateurs de services essentiels » et certains fournisseurs de services numériques seront bien soumis à des exigences de sécurité et de notification d'incidents de sécurité.

### Sécuriser les infrastructures

Du côté des fournisseurs de services numériques, les places de marché en ligne, les moteurs de recherche et les fournisseurs de services de Cloud actifs dans l'UE sont concernés. Ils devront prendre des mesures pour « assurer la sécurité de leur infrastructure » et signaler « les incidents majeurs » aux autorités nationales. Mais les exigences auxquelles devront se plier ces fournisseurs, seront moins élevées que celles applicables aux opérateurs de services essentiels.

Publication de la Directive NIS au Journal officiel de l'Union européenne Adoption de la directive NIS : l'ANSSI, pilote de la transposition en France

Denis Jacopini anime des **conférences et des formations** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons conférences et formations pour sensibiliser décideurs et utilisateurs aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur

: https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- · Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés);
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Original de l'article mis en page : Directive NIS adoptée: quelles conséquences pour les entreprises?

## Certification des objets connectés de santé - Web des Objets



### De l'objet connecté de bien-être à l'objet connecté de santé : une certification qui a du sens

Très répandus sur le marché, les objets connectés de bien-être ont pour vocation de développer un état de satisfaction morale ou physique, sans obligation de mesurabilité ni de résultats cliniques. Les données de bien-être peuvent être observées sur le long terme pour mieux déterminer l'état de santé d'un patient. De nombreux objets connectés de santé sont en développement, afin de fournir des données quantifiables et médicalement fiables. L'usage de ces objets se fait notamment dans un but nommé le « quantified self ». C'est une collaboration entre utilisateurs et fabricants d'outils qui partagent un intérêt pour la connaissance de soi à travers la mesure et la traçabilité de soi. Des objets connectés tels que la balance Polar connectée pour suivre son poids ou le capteur Withings Go permettant de mesurer son activité physique et de suivre ses cycles de sommeil sont des outils qui s'intégrent dans cette démarche.

La frontière entre les domaines du bien-être et de la santé va s'estomper. L'objectif est que demain, les gens disent que c'est eux qui prennent soin de leur santé, avec l'aide de leur médecin et no lus leur médecin seul. Le patient devient expert, le médecin va devoir le prendre comme un partenaire. » édric Hutchings, PDG de Withings (Cahiers IP n°2 : Le corps, nouvel objet connecté).

L'objet connecté de santé en tant que dispositif médical, qu'est-ce que c'est ? Les objets connectés de santé sont classés dans la catégorie des dispositifs médicaux pour l'ANSM et la CNIL. Adrien R . Rousseaux, expert en protection des données à caractère privé à la CNIL, apporte des

éléments permettant de mieux comprendre les enjeux de la certification.
Selon l'ANSM, est considéré comme dispositif médical « tout instrument, appareil, équipement, logiciel, matière ou autre article, utilisé seul ou en association, y compris le logiciel destiné par le Seton L MASA, est Constance Comme dispositir medical « Your instrument, appareir, equipment, toglicet, matrier ou autre afficte, untilse seut ou en association, y compins te toglicet restricted after untilsé after utilisé after utilisé after utilisé spécifiquement à des fins diagnostique et/ou thérapeutique, récessaire au bon fonctionnement de celui-ci. Le dispositif médical est destiné par le fabricant à être utilisé chez l'homme à des fins de diagnostic, prévention, contrôle, traitement ou atténuation d'une maladie, d'une blessure ou d'un handicap ; mais aussi d'étude ou de remplacement ou modification de l'anatomie ou d'un processus physiologique. Son action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais sa fonction peut être assistée par de tels moyens » (directive européenne 93/42/CEE).

\*\*Pour la CNIL, c'est l'utilisation ou l'exploitation des données recueillies par les objets connectés de santé, ou de bien être, qui fait intervenir la loi Informatique et Libertés.

Il n'y a pas de définition dans la loi française d'une donnée de santé permettant de la distinguer de la donnée de bien-être. Mais le règlement européen relatif à la protection des données personnelles, adopté le 14 avril dernier, et qui sera applicable en 2018, apporte une définition légale qui toutefois n'est pas opposable (ne peut être utilisée comme argument juridique) mais le sera d'ici son application. L'article 4 de ce règlement européen définit les données de santé comme « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris les rrestations de services, de soins de santé qui révèlent des informations sur l'état de santé de cette personne.

Des objets connectés de santé sont déjà commercialisés en tant que dispositifs médicaux.

Le Tensiomètre Bluetooth de Withings se connecte aux smartphones et mesure la pression systolique, diastolique ainsi que le rythme cardiaque. Cet appareil a obtenu la certification européenne CE, il est donc certifié comme dispositif médicau.

L'électro-stimulateur connecté MyTens de BewellConnect développé avec le laboratoire Visiomed se connecte aux smartphones et stimule des zones précises du corps avec des électrodes pour réduire les

douleurs. Il est remboursé par la sécurité sociale, donc reconnu comme dispositif médical.

MyECG, l'électrocardiogramme connecté de BewellConnect développé avec le laboratoire Visiomed se connecte au smartphone et mesure la fréquence cardiaque. Il a reçu le marquage CE, ce qui en fait également un dispositif médical certifié.







Quelles étapes pour certifier un objet de santé, dispositif médical ? Afin de certifier un objet connecté comme dispositif médical, le fabricant doit d'abord constituer un d dossier auprès d'un organisme notifié. Ce dernier évalue la conformité aux exigences essentielles et un objet connecté comme disp cat européen de marquage CE. délivre le certificat

La donnée de santé cible un risque de maladie. Les données issues d'un dispositif médical certifié peuvent être utilisées par un professionnel de santé. Les formalités auprès de la CNIL ne sont pas les La donnée de santé cible un risque de maladie. Les données issues d'un dispositif médical certifié peuvent être utilisées par un professionnel de santé. Les formalités auprès de la CMIL ne sont pas les mêmes pour un traitement de données de bien-être et un traitement de données de santé. En effet, les données de santé sont distes "ensibles" d'après l'article 8 de la loi Informatique et Libertés. Pour un objet connecté de bien-être, ne comportant donc pas de données de santé ou pour lequel le consentement de l'utilisateur est demandé, les formalités sont déclaratives. Même si le traitement des données doit respecter la loi Informatique et Libertés (notamment le respect des droits des personnes à pouvoir s'opposer, à pouvoir rectifier ou tout simplement à pouvoir être informé et la mise en place de mesures de sécurité adaptées), l'entreprise doit simplement signaler les modalités d'usage à la CMIL Pour les objets connectés de santé, ou de bien-être utilisant des données de santé, les formalités nécessitent une autorisation de la CMIL avant de pouvoir proposer le service délivré par l'objet connecté. En moyenne, les procédures prennent de 2 à 6 mois selon la disponibilité du responsable de traitement. Ce dernier est la personne ou l'entité qui définit le service proposé par un dispositif médical, et donc qui gère la transmission de données générées par ce dispositif médical à un serveur, le stockage des données, etc. Un certain nombre d'informations sont à fournir à l'usage d'après l'article 32 de la loi informatique et Libertés. « La personne auprès de laquelle sont recueillies les données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable de traitement (ou son représentant :

\*\*Ne l'identifié du responsable de traitement (oui va effectuer les traitements sur les données)

De l'identité du responsable de traitement (qui va effectuer les traitements sur les données)

- Des finalités poursuivies par le traitement
  Du caractère obligatoire ou facultatif des réponses
  Des conséquences éventuelles d'un défaut de réponses (par exemple le service ne pourra pas être rendu dans son intégralité)
- Des destinataires ou catégories de destinataires des données Des droits de l'utilisateur sur ces données »

se un générateur de mentions "informatique et libertés" équivalent aux

Les intérêts de la certification pour l'utilisateur et le distributeur
Toutes ces démarches visent à protéger l'utilisateur de tout mésusage des dispositifs médicaux. C'est cette « digitalovigilance » qui garantit une communication maîtrisée des données de santé aux personnes souhaitées. L'usager ayant enregistré des données doit avoir connaissance des destinataires s'il y a transmission et il doit pouvoir maîtriser à qui il envoie quelles données.

Sur de nombreux apparells, le système d'APT (Application Programming Interface = interface pour l'accès programmé aux applications) permet à l'utilisateur de partager la donnée qui a été générée par un capteur avec un nouveau service, une application. Il peut à tout moment déconnecter les applications pour que les données cessent d'être transmises.

De nombreuxes données transmises par les dispositifs médicaux peuvent être très utiles, dans le cadre de la recherche notamment. L'intérêt majeur de la certification des données de santé est donc qu'elles peuvent être utilisées par des professionnels de santé. De plus, un objet certifié dispositif médical peut être vendu en pharmacie : il peut être prescrit par un professionnel de santé et donc

Bluetens et Beta-bioled : deux objets connectés vers la certification





Électrostimulateur connecté Bluetens / Test sanguin portable connecté Beta-Bioled

Liectrostimulateur connecte Bluetens d'evelopé un délectrostimulateur connecte Bluetens advelopé un délectrostimulateur connecté pour soulager la douleur et se relaxer. Son objectif premier est de créer un objet de santé qui se définit par sa fonction et son utilité. Il doit apporter plus que de l'analyse ou de la collecte de données. L'objectif est un réel changement d'état de l'utilisateur, l'objet doit avoir un impact remarquable sur la santé. L'électrostimulateur Bluetens est certifié ISO 13485 par une société de certification qui effectue un audit d'une part auprès de l'entreprise Bluetens, et d'autre part sur l'objet connecté de santé. Dans ce cas, c'est l'entreprise allemande TÜV agréée par les autorités européennes qui a certifié l'objet. L'ISO 13485 atteste que l'entreprise Bluetens respecte bien les normes nécessaires à l'élaboration de dispositifs médicaux. Cet appareil est donc certifié d'utilité médicale. Le but de l'entreprise étant de le distribuer le plus largement possible, il est vendu dans les enseignes de grande distribution spécialisées telles que Darty ou la Fnac.

De son côté, la société Archimej Technology est en train de développer Beta-Bioled, un test sanguin portable et connecté. Cette entreprise cherche à insérer sur le marché des dispositifs médicaux e De son côté, la société Archinej Technology est en train de développer Beta-Bioled, un test sanguin portable et connecté. Cette entreprise cherche à insérer sur le marché des dispositifs médicaux en franchissant toutes les étapes de la certification jusqu'à obtenir les agréments de la Seurité sociale pour que l'appareil puisse être remboursé. Cette démarche s'inscrit dans une volonté d'asseoir la crédibilité de Beta-Bioled face aux utilisateurs et au corps médical. Le processus de certification passe ici par 3 étapes dont la première est la formation auprès d'organismes spécialisés. Le biocluster Genopole leur apporte les conseils sur les questions des biotechnologies et Médicen facilite l'insertion d'innovations dans le domaine de la santé humaine vers les marchés industriels. La secondé étape une fois l'Objet conceptualisé et réalisé, consiste à réaliser des essais cliniques avec quelques milliers de tests dans des structures médicales. Enfin, l'Objet sera certifié uniquement lorsque la Haute Autorité de Santé (HAS) aura validé toute la procédure. Et pour assurer une diffusion optimale dans le parcours médical, Archimej Technology souhaite obtenir l'agrément LPPR (Liste des Produits et Prestations Remboursables), qui permettra un remboursement de Beta-Bioled par l'Assurance Maladie. Ce parcours du combattant assurant une crédibilité et une valeur médicale peut prendre plusieurs années : l'objectif de mise sur le marché est fixé à 2018. En premier lieu, il sera distribué aux professionnels de santé (urgences, SAMU, maisons de retraite.). Ensuite la vente sera ouverte au grand public pour les malades chroniques, invalides légers ou séniors ne pouvant se déplacer en laboratoires. A terme l'objectif est de cibler les pharmacies comme canaux de distribution.

Article original de Charles Deyrieux



- Expertises de systèmes de vote électronique
- Formations et conférences en cybercrim
- Formation de C.I.L. (Correspondants Informatique t Libertés);
- Accompagnement à la mise en conformité CNIL de votre établissement.



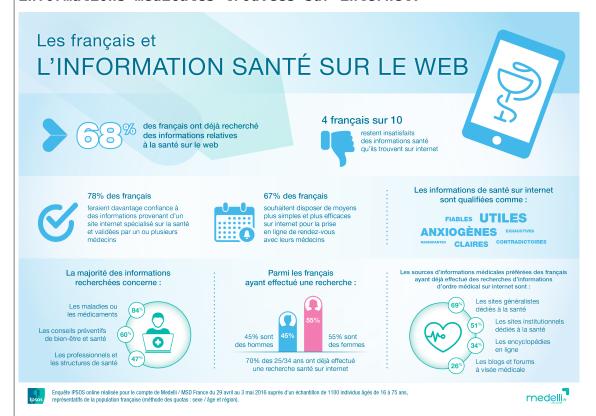
Original de l'article mis en page : Certification des objets connectés de santé — Web des Objets

### Usages et attentes des Français à l'égard du digital en matière d'information sur leur santé

6



Dans un monde de santé de plus en plus connecté et digitalisé, 4 français sur 10 restent insatisfaits des informations santé qu'ils trouvent sur internet. A la veille du lancement par le laboratoire pharmaceutique MSD d'une nouvelle plateforme digitale d'information médicale, le groupe et Ipsos se sont intéressés aux usages et attentes des Français à l'égard des informations médicales trouvées sur internet.



### Article original de Ipsos



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- · Expertises de systèmes de vote électronique ;
- · Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés);
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Original de l'article mis en page : Usages et attentes des Français à l'égard du digital en matière d'information sur leur santé