Cybersécurité et RGPD

ASC2SI
LA RÉSILIENCE DE VOTRE SYSTÈME

URPS médecins libéraux
Auvergne Rhône Alpes

Plan de la présentation

- Qui suis je ?
- Sécurité Informatique
  - Les bonnes pratiques de l'ANSSI
  - La sécurité au Cabinet
- LE RGPD dans la Santé
  - Retour après 1 an d'application
  - Comment s'y conformer

Présentation d’ASC2SI

ASC2SI

LA RÉSILIENCE DE VOTRE SYSTÈME

Expertise en Cyber-sécurité

Nos références RGPD

GHT LOIRE
Groupement Hospitalier de Territoire
« Des femmes et des hommes au service de votre santé »

DEPISTAGE DES CANCERS
Centre de coordination
Auvergne-Rhône-Alpes

STDV
SANTÉ TRAVAIL DRÔME VERCORS

ALPHA ROUTAGE
Le spécialiste de vos mailings
- www.alpharoutage.fr -

Loire
LE DÉPARTEMENT

CSI
CASH SYSTEMES INDUSTRIE

Nos références RGPD

L'ATELIER RGPD

ATTESTATION DE SUIVI

La Commission Nationale de l'Informatique et des Libertés (CNIL) atteste que **M. Sébastien CLAUDE** a suivi avec succès les cours des quatre modules du **MOOC L'Atelier RGPD** et obtenu les scores suivants aux évaluations :

MODULES	DATE DE L'ÉVALUATION	SCORE
LE RGPD ET SES NOTIONS CLÉS	11/03/2019	90%
LES PRINCIPES DE LA PROTECTION DES DONNÉES	19/03/2019	90%
LES RESPONSABILITES DES ACTEURS	19/03/2019	90%
LE DPO ET LES OUTILS DE LA CONFORMITÉ	19/03/2019	90%

Fait le 02 Mai 2019

CNIL.

ASC2SI
LA RÉSILIENCE DE VOTRE SYSTÈME

Création d'entreprise

Dirigeant EURL ASC2SI · Firminy (France) · depuis 03/2018

ITS Group

ENEDIS
L'ELECTRICITE EN RESEAU

Directeur de Projets – Solutions de Sécurité et Filtrage Applicatif

Responsable de Centre de Compétence · Lyon (France) · CDI ·12/2016 à 01/2018

Hôpital Le Corbusier Firminy

Responsable du Système d'information/ RSSI et CIL

Hôpital Le Corbusier· Firminy (France) · CDI · 09/2008 à 12/2016

Sécurité Informatique

#CyberSecurityMonth

Sécuriser les dossiers

- Sécuriser les documents papiers et informatiques
- Sauvegarder les données et les externaliser
- Verrouiller les ordinateurs automatiquement
- Ne pas laisser une personne seule avec la possibilité de consulter les dossiers
- Les personnels administratifs ne doivent pas avoir accès aux données médicales
- S’assurer que les prestataires n’accèdent pas aux données
- Utiliser des Outils sécurisés pour échanger entre Professionnels de Santé

La gestion des mots de passe

- utilisation d'un mot de passe conforme aux recommandations de la CNIL, 12caractères (chiffres, lettres majuscules et minuscules, caractères spéciaux), renouvelé régulièrement ;
- Exemple Une Phrase mémorisable : *J'ai acheté mon chien à Jardiland le 25/01/2015 =>J'aAmCàJl25-01-15*

Les autres mesures indispensables

- **verrouillage** de votre session informatique **automatiquement** après maximum 30 minutes d'inactivité ;
- **antivirus** à jour, pare-feu, application systématique des correctifs de sécurité du système informatique et des logiciels ;
- **sauvegardes** régulières des données (sauvegarde au minimum hebdomadaire, avec conservation des sauvegardes mensuelles sur 12 mois glissants) et leur conservation dans un lieu différent que votre cabinet ;
- chiffrement des données avec un logiciel adapté ;
- absence ou minimisation des connexions d'appareils non professionnels sur le réseau ;
- authentification via votre **Carte de professionnel de santé** (CPS) ou tout moyen alternatif d'authentification forte

Les outils de l'URPS

- Les 12 bonnes pratiques de la sécurité inf ormatique
- FICHE sur la cybersécurité et le RGPD

https://www.cyberveille-sante.gouv.fr/

ANSSI Agence nationale de la sécurité des systèmes d'information

CNIL.

Cybercriminalité

Le *Guide des bonnes pratiques de l'informatique* édité notamment par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) présente douze recommandations qui constituent un corpus incontournable.

1 hoisir avec soin ses mots de passe

Les mots de passe doivent être difficiles à retrouver à l'aide d'outils automatisés ou à deviner. Pour cela, ils doivent comporter **douze caractères de type différent** (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien avec l'utilisateur (nom, date de naissance...) et ne figurant pas dans le dictionnaire.

Au sein de l'entreprise, il convient de :

1. Déterminer des règles de choix et de dimensionnement (longueur) des mots de passe et de... les faire respecter ;
2. Modifier toujours les éléments d'authentification (identifiants, mots de passe) définis par défaut sur les équipements (imprimantes, serveurs...) ;
3. Ne pas conserver les mots de passe dans des fichiers ou sur des post-it ;
4. Sensibiliser les collaborateurs au fait qu'ils ne doivent pas pré-enregistrer leurs mots de passe dans les navigateurs.

2 Mettre à jour régulièrement ses logiciels

Dans chaque système d'exploitation (Android, IOS, Windows...), logiciel ou application, des vulnérabilités existent.
Une fois découvertes, elles sont corrigées par les éditeurs qui proposent des mises a jour de sécurité. Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les hackers exploitent ces vulnérabilités pour mener à bien leurs attaques.

Au sein de l'entreprise, il convient de :

1. Définir et faire appliquer par l'équipe une politique de mises à jour régulières ;
2. Configurer les logiciels de la société ou du cabinet pour que les mises à jour de sécurité s'installent automatiquement et, à défaut, de télécharger les correctifs de sécurité disponibles ;
3. Utiliser exclusivement les sites Internet officiels des éditeurs.

URPS médecins libéraux Auvergne Rhône Alpes

3

Bien connaître ses utilisateurs et ses prestataires

Lors de l'utilisation quotidienne de son ordinateur, on ne se sert que du compte utilisateur. Le compte administrateur, lui, n'est à utiliser que pour intervenir sur le fonctionnement global de l'ordinateur (gérer des comptes utilisateurs, modifier la politique de sécurité...).
Les systèmes d'exploitation récents permettent d'intervenir facilement sur le fonctionnement global d'une machine sans changer de compte. Le mot de passe administrateur est simplement demandé pour effectuer les manipulations désirées. Le compte administrateur permet d'effectuer d'importantes modifications sur votre ordinateur.
Au sein de l'entreprise, il est impératif de :

1. Réserver l'utilisation du compte administrateur au service informatique si celui-ci existe, sinon d'en protéger l'accès en n'ouvrant pour les employés que des comptes utilisateur ;
2. Identifier les différents utilisateurs du système et les droits qui leur sont accordés ;
3. Supprimer les comptes anonymes et génériques (stagiaire, presse...), chaque utilisateur devant être identifié nommément afin de pouvoir relier une action sur le système à un utilisateur ;
4. Encadrer par des procédures les arrivées et les départs de personnels pour s'assurer que les droits octroyés sur les systèmes d'information sont appliqués au plus juste et qu'ils sont révoqués lors du départ de la personne.

URPS médecins libéraux Auvergne Rhône Alpes

4

Effectuer des sauvegardes régulières

Pour sauvegarder ses données, on peut utiliser des supports externes (disque dur externe réservé exclusivement à cet usage…) que l'on range ensuite dans un lieu éloigné de l'ordinateur, de préférence à l'extérieur du siège social pour éviter que la destruction des données d'origine ne s'accompagne de la destruction de la copie de sauvegarde en cas d'incendie ou d'inondation, ou que la copie de sauvegarde ne soit volée en même temps que l'ordinateur.

URPS médecins libéraux Auvergne Rhône Alpes

5

Sécuriser l’accès Wi-Fi de votre entreprise

Un Wi-Fi mal sécurisé peut permettre à des personnes d’intercepter vos données et d’utiliser la connexion Wi-Fi à votre insu pour effectuer des opérations malveillantes.

C’est pourquoi l’accès à Internet par un point d’accès Wi-Fi est à éviter dans le cadre professionnel : une installation filaire est plus sécurisée et plus performante. Si le Wi-Fi est le seul moyen possible d’accéder à Internet, il convient de sécuriser l’ensemble en configurant la borne d’accès à Internet, notamment en modifiant la clé de connexion par défaut par une clé (mot de passe) de plus de douze caractères de types différents.

6

Être aussi prudent avec son ordiphone ou sa tablette qu'avec son ordinateur

Les ordiphones (Smartphones) sont très peu sécurisés.

Il est donc indispensable :

1. De n'installer que les applications nécessaires et vérifier à quelles données elles peuvent avoir accès avant de les télécharger ;
2. En plus du code PIN qui protège la carte téléphonique, utiliser un schéma ou un mot de passe pour sécuriser l'accès au terminal et le configurer pour qu'il se verrouille automatiquement ;
3. Effectuer des sauvegardes régulières des contenus sur un support externe ;
4. Ne pas pré-enregistrer les mots de passe.

Protéger ses données lors de ses déplacements

Voyager avec des appareils nomades fait peser des menaces sur des informations sensibles en cas de vol ou de perte.

Il convient donc de n'utiliser que du matériel dédié à la mission et ne contenant que les données nécessaires, ou encore d'éviter de connecter ses équipements à des postes qui ne sont pas de confiance.

Autre précaution : ne jamais utiliser les clés USB offertes lors des déplacements car elles sont susceptibles de contenir des programmes malveillants.

Être prudent lors de l'utilisation de sa messagerie

Les courriels et leurs pièces jointes jouent un rôle central dans les attaques informatiques. Des précautions sont donc à prendre :

1. Vérifier la cohérence entre l'expéditeur présumé et le contenu du message et vérifier son identité ;
2. Ne pas ouvrir les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents ;
3. Si des liens figurent dans un courriel, passez votre souris dessus avant de cliquer. L'adresse complète du site s'affichera dans la barre d'état du navigateur, ce qui permet d'en vérifier la cohérence ;
4. Ne jamais répondre par courriel à une demande d'informations personnelles ou confidentielles car il s'agit d'attaques par hameçonnage ;
5. Ne pas ouvrir ni relayer des messages de types alerte virale, etc. ;
6. Désactiver l'ouverture automatique des documents téléchargés et lancer une analyse antivirus avant de les ouvrir.

9 Télécharger ses programmes sur les sites officiels des éditeurs

Télécharger du contenu numérique sur des sites Internet dont l'origine n'est pas assurée, c'est prendre le risque d'enregistrer sur son ordinateur des programmes ne pouvant être mis à jour et qui, le plus souvent, contiennent des virus ou des chevaux de Troie.
Dans ce contexte, il est recommandé de :

1. Télécharger les programmes sur les sites de leurs éditeurs ou d'autres sites de confiance ;
2. Décocher ou désactiver toutes les cases proposant d'installer des logiciels complémentaires ;
3. Réfléchir avant de cliquer sur des liens sponsorisés ; désactiver l'ouverture automatique des documents téléchargés et lancer une analyse antivirus avant de les ouvrir.

10 Etre vigilant lors d'un paiement sur Internet

Avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications.
Dans ce contexte, il est recommandé de :

1. Contrôler la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet ;
2. S'assurer que la mention « https:// » apparaît au début de l'adresse du site Internet ;
3. De vérifier l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe ;
4. Privilégier la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS ;
5. Ne jamais transmettre le code confidentiel de sa carte bancaire.

11 Séparer les usages personnels des usages professionnels

Il est recommandé de :

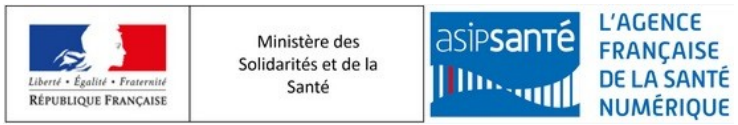
1. ne pas faire suivre ses messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles ;
2. ne pas héberger des données professionnelles sur des équipements personnels ou sur des moyens personnels de stockage en ligne ;
3. éviter de connecter des supports amovibles personnels aux ordinateurs de la structure professionnelle.

Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

Les données que l'on laisse sur Internet nous échappent instantanément. D'où la plus grande prudence dans la diffusion d'informations personnelles sur le Net.

Par exemple, en décochant les cases qui autoriseraient le site à conserver ou à partager ses données ou en utilisant plusieurs adresses électroniques dédiées à ses différentes activités (sérieuses ou autres) sur Internet.

www.CYBERVEILLE-sante.gouv.fr



- **ASIP Santé**
  Cellule d'accompagnement cybersécurité des structures de santé (ACSS) depuis 10/2017, sous la responsabilité du fonctionnaire en charge de la sécurité des systèmes d'information (FSSI) du ministère, Philippe Loudenot.

- **Service national de cybersurveillance en santé d'ici 2020.** Délégation ministérielle du numérique en santé et de l'Agence du numérique en santé (ANS).

- **La cellule ACSS** assure une veille sur l'actualité des systèmes d'information et sur les menaces présentes sur le secteur de la santé sur le site cyberveille-sante.gouv.fr

- La plupart des failles de sécurité s'expliquaient par un **« manque de vigilance »** et une **« méconnaissance »** des règles de cybersécurité des systèmes d'information.

URPS médecins libéraux Auvergne Rhône Alpes

Cybersécurité

Le Guide des bonnes pratiques de l'informatique édité notamment par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) présente **12 recommandations** qui constituent un corpus incontournable.

1. **Choisir des mots de passe composés de chiffres & de lettres (dont des majuscules) et penser à les changer régulièrement. Varier les mots de passe.**
2. **Mettre régulièrement à jour ses logiciels de sécurité (antivirus et pare-feu).**
3. **Contrôler les accès des utilisateurs et prestataires.**
4. **Effectuer des sauvegardes régulières, les vérifier et les stocker sur disque dur externe déposé à l'extérieur du cabinet.**
5. **Sécuriser l'accès Wi-Fi de votre cabinet (voire le désactiver - Est-il vraiment nécessaire ?).**
6. **Être aussi prudent avec son smartphone ou sa tablette qu'avec son ordinateur.**
7. **Protéger ses données lors de ses déplacements. Être extrêmement vigilant lors de l'utilisation d'un Wi-Fi public.**
8. **Être précautionneux lors de l'utilisation de sa messagerie : déposer les pièces jointes sur le disque dur avant de les ouvrir (elles seront ainsi analysées par l'antivirus), vérifier l'adresse de l'expéditeur…**
9. **Télécharger ses programmes sur les sites officiels des éditeurs.**
10. **Être vigilant lors d'un paiement sur Internet : est-ce un site sécurisé ? Le https et un cadenas doivent apparaître dans l'adresse du site. N'utiliser que les sites bancaires pour faire vos achats.**
11. **Séparer les usages personnels des usages professionnels. Rédiger une charte informatique à faire signer par les collaborateurs et employés.**
12. **Prendre soin de ses informations personnelles, professionnelles et de son identité numérique.**

RGPD

Règlement Général sur la Protection des Données personnelles

URPS médecins libéraux Auvergne Rhône Alpes

Les six points européens

- Redéfinition du consentement
- Des données supprimées lorsqu'elles deviennent obsolètes
- Minimisation et restriction du traitement des données
- Intégrité des données
- Confidentialité
- Risques encourus en cas de non-respect du Règlement

Les obligations des médecins

- **Le dossier médical** : Respecter les obligations de fond, mettre en place un registre (exemple : https://bit.ly/2LrGmJS), sécuriser l'accès aux données, veiller à la durée de conservation des données...
- **La prise de rendez-vous** : Mêmes obligations que pour les dossiers (limitation du recueil d'informations, tenue à jour des traitements).
- **La messagerie électronique** : Utiliser les messageries sécurisées lors des échanges d'informations avec les professionnels de santé.
- **Les smartphones et tablettes** : Veiller à ce que l'accès aux applications médicales soit sécurisé, éviter de stocker des données sur ces outils.
- **La télémédecine** : Toute séance de télé-consultation doit passer par des outils sécurisés.
- **Les objets connectés** : S'interroger sur le cryptage, l'hébergement et la sécurisation de ses accès, le traitement des données...

Pour en savoir plus, consultez le site de l'URPS Médecins
[CYBERSÉCURITÉ] http://bit.ly/2tuPZ2y ET [RGPD] http://bit.ly/2znd9ya

Consultez et téléchargez les fiches d'alerte gendarmerie disponibles à cette adresse :
http://www.ene.fr/informer/ressources-documentaires1/fiches-alertes-gendarmerie.html

urps@urps-med-aura.fr

URPS Médecins Libéraux Auvergne-Rhône-Alpes
20, rue Barrier 69006 LYON ~ 04 72 74 02 75
24, allée Évariste Galois 63170 AUBIÈRE ~ 04 73 27 77 44

URPS médecins libéraux Auvergne Rhône Alpes

L'URPS Médecins AuRA vous invite à une **conférence-débat**

PROTÉGEZ VOTRE EXERCICE LIBÉRAL

CYBERSÉCURITÉ

RGPD

- Protection des données de santé numériques
- Les 12 bonnes pratiques de la sécurité informatique : comment sécuriser son poste
- Le RGPD, Réglement Général sur la Protection des Données pour les médecins

Intervention de M. Sébastien CLAUDE, consultant, expert en cybersécurité, des docteurs Eric TEIL et Didier ANNE, URPS Médecins Libéraux AuRA

Jeudi 6 juin 2019 de 19h à 21h30

Dans les locaux de l'URPS Médecins Libéraux AuRA
24 Allée Évariste Galois à **Aubière**
(Parc Technologique de la Pardieu)

19h : Accueil et Buffet
20h à 21h15 : Conférence
21h15 à 21h30 : Questions

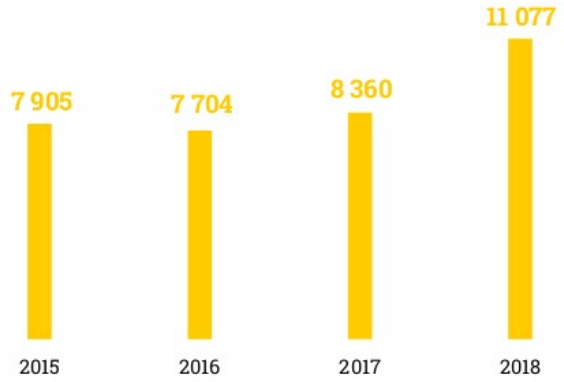
Merci de confirmer votre présence : 04 72 74 02 75

Merci de votre attention

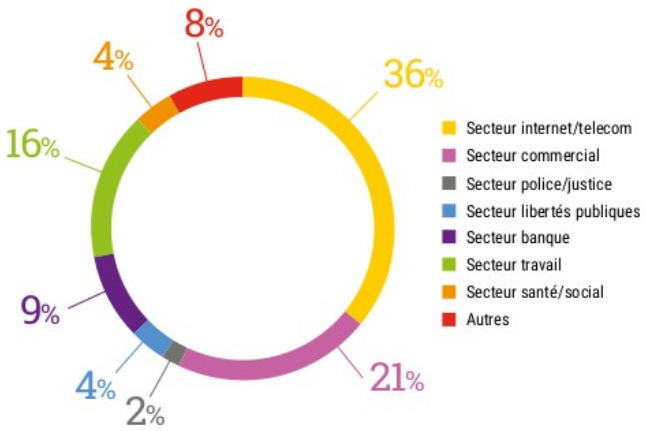
Le RGPD appliqué au monde des médecins libéraux

RGPD déjà 1 an

Évolution du nombre de plaintes depuis 2015



Répartition des plaintes par secteur d'activité (2018)



53 000

ORGANISMES ONT DÉSIGNÉ UN DÉLÉGUÉ

Soit 19 000 Délégués physiques par l'effet mutualisation

RGPD Les grandes lignes

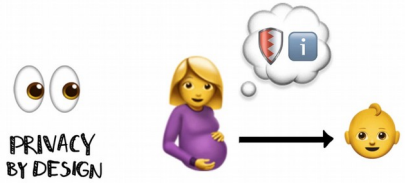
- Un Règlement **Européen** applicable depuis 25/05/2018
- Réaliser un **registre des Traitements** de données personnelles
- Notifier les Violations de données : Accès illégitimes, Perte d'intégrité et effacement de données **=> 72H**
- Permettre aux personnes d'**exercer leurs droits** : accès, rectification, oubli, portabilité , opposition…
- Réaliser des **AIPD (Analyse d'Impact sur la Protection des données)**

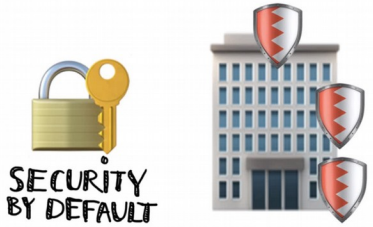
CNIL.

=>Des sanctions allant jusqu'à 4 % du CA

RGPD Les autres principes

- Accountabillity = partage de la responsabilité
- privacy by design et de security by default





- Analyse d’impact = Privacy Impact Assessment: PIA/AIPD

CNIL.

Comment s’y conformer

Les Traitements en Santé

- Réaliser son registre
- Informer ses patients et le personnel
- Mettre en place l’organisation et la sécurité des DCP (Données à caractère personnel)
- Réaliser les AIPD
- Sécuriser son SI (Système d’Information)
- Minimiser les données
- Respecter les durées de conservation définies

Réalisation du Registre

- ***Qui ? ; Quoi ? ; Pourquoi ? ; Où ? ; Jusqu'à quand ? ; Comment ?***
- ***Prioriser les traitements***
- ***Tenir le registre à jour***
-

Identification du traitement				Acteurs	Finalité du traitement	Transferts hors UE ?	Données sensibles ?	Pôle de rattachement	Direction concernée	Mission de service Public		Métrique pour le Tableau de bord						
Nom / sigle	N° / REF	Date de création	Dernière mise à jour	Responsable du traitement	Finalité principale	Transferts hors UE ?	Données sensibles ?	Pôle de rattachement	Direction concernée	Licéité du TTT	Module d'application	Date de dernière révision > 1an	Catégorie de Personne	Volumétrie	Type de DCP	Criticité des DCP	Présence de DCP Sensibles	PIA Nécessaire	Poids Calculé
Gestion Administrative du Patient		20/09/2018	20/09/2018	Responsable du bureau des entrées	Assurer la prise en charge administrative puis médicale d'un patient	Oui	Oui			Mission d'intérêt public			Patients	3	(20) Données concernant la santé	20		Oui	60
Gestion de l'impression des badges d'accès au site		20/09/2018	20/09/2018	Responsable du service Technique	gérer les cartes d'identification des agents	Non	Non			Intérêts légitimes			Agents	2	(5) Etat civil, identité, données d'identification, images...	5		Non	10
Gestion du dossier patient informatisé		20/09/2018	20/09/2018	Direction de l'information médicale	Dossier patient informatisé	Non	Oui			Sauvegarde des intérêts vitaux de la personne			Patients	3	(20) Données concernant la santé	20		Oui	60
Dossier patient de Biologie		20/09/2018	20/09/2018	Chef de service du plateau de biologie	mettre à disposition des médecins pour diagnostique les réultats des analyse biologique effectué pour un patient	Non	Oui			Sauvegarde des intérêts vitaux de la personne			Patients	3	(20) Données concernant la santé	20		Oui	60

Les Traitements en Santé

- DPI
- Gestion des prescriptions : Biologies, Examens, Médicaments
- Dossier patients partagé (Régionaux)
-
- Le personnel : GRH,...
-
- Gestion des commandes :
-
- Sécurisation des locaux(vidéosurveillance,..)

Les Patients

AIPD

Les Employés

AIPD

Les fournisseurs

SI DPI hébergé

Comment Informer les patients

- Une Affiche en salle d’attente
- Si des prestataires externes interviennent :
  - Information dédiée lors de la consultation
- Si prise de rendez-vous en ligne
  - Vérifier la présence des informations sur le site

Bon à savoir

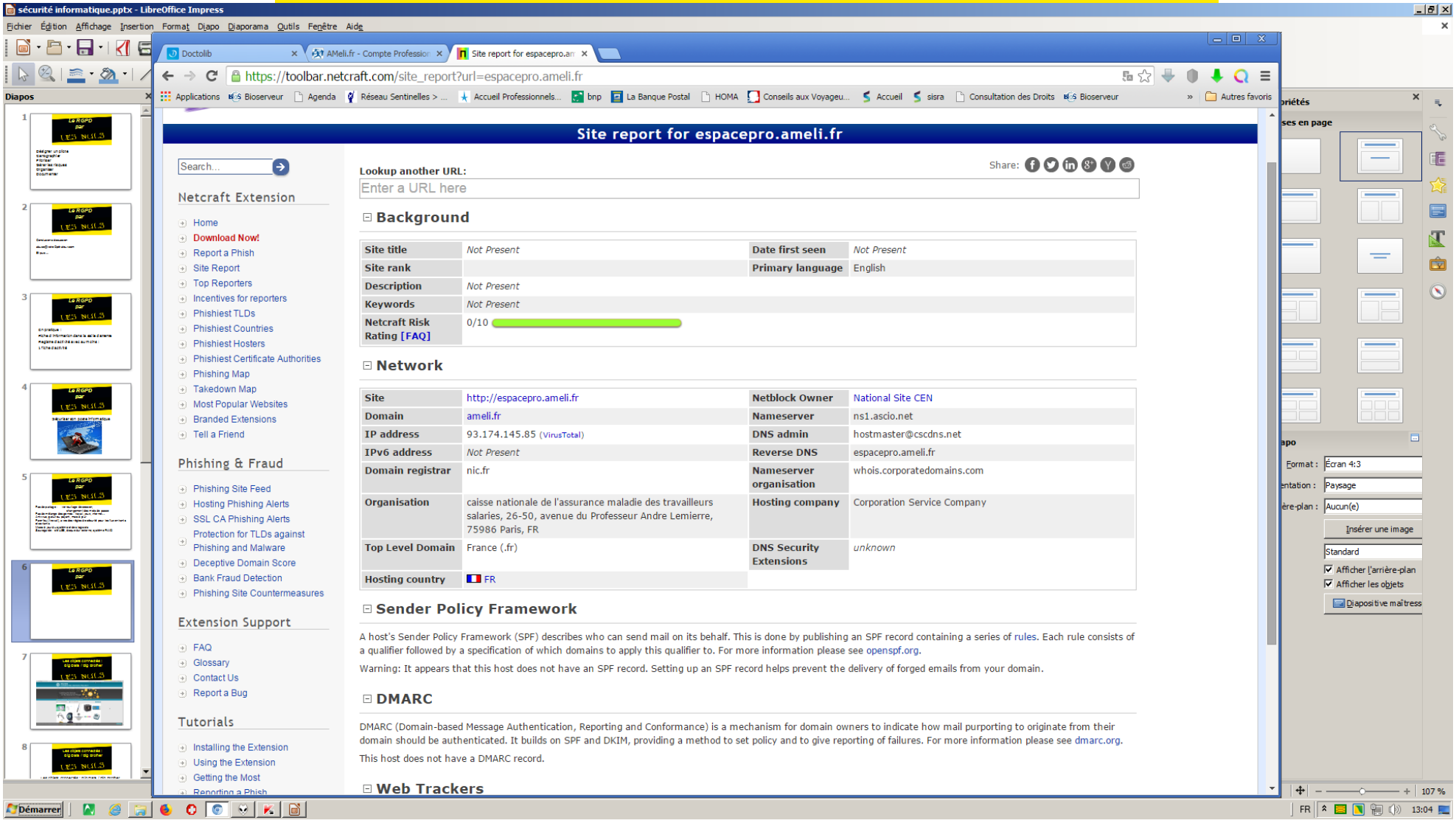
La personne a le droit de **s’opposer à tout moment à un échange ou un partage d’informations** la concernant.

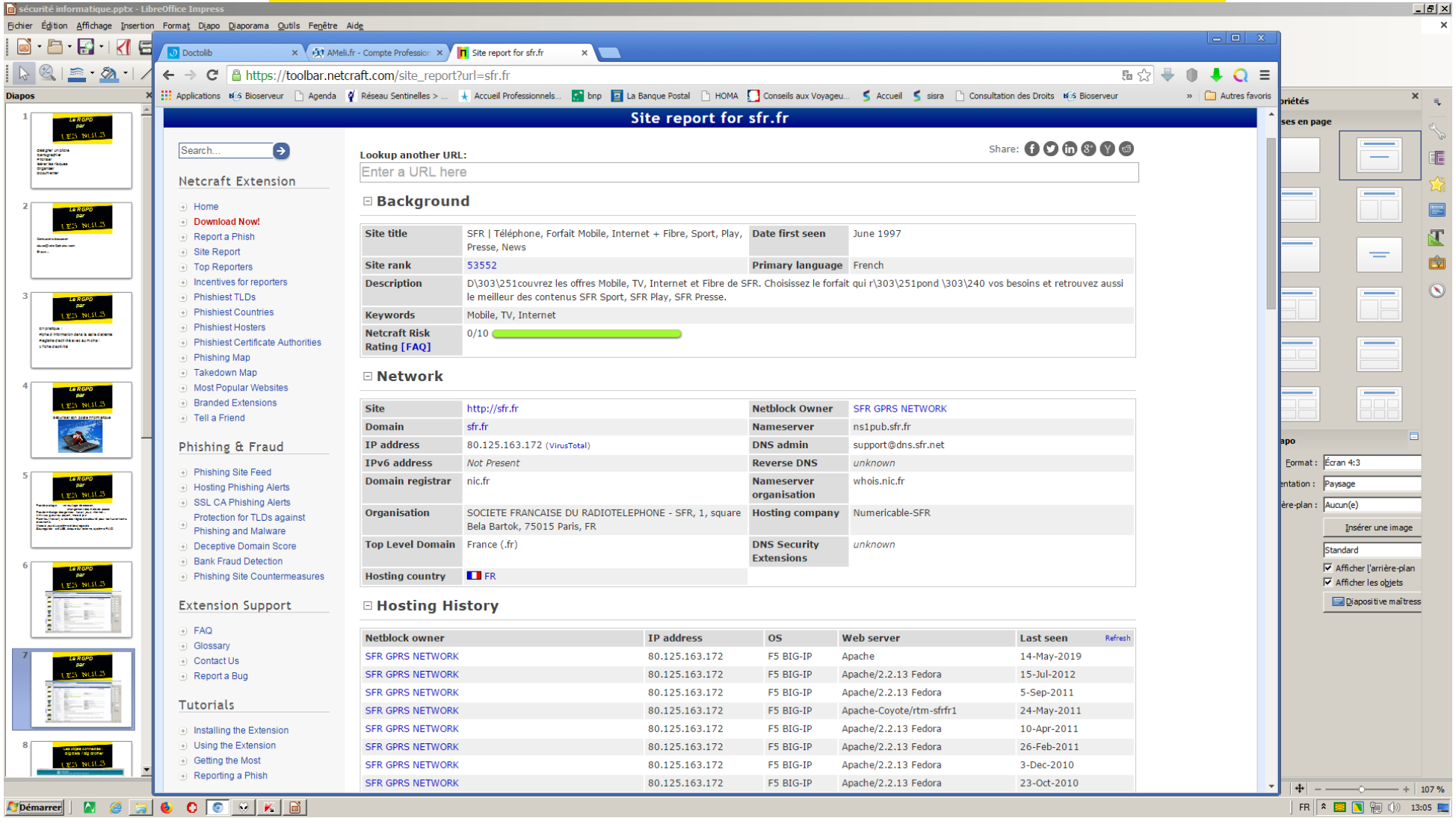
- En pratique :
- Fiche d’information dans la salle d’attente
- Registre d’activité avec au moins :
- 1 fiche d’activité

Le RGPD par LES NULS

Sécuriser son poste informatique

Pas de partage : verrouillage de session,
changement des mots de passe
Pas de mélange des genres : travail, jeux, internet…
Antivirus, gatuit ou payant, mais à jour
Pare-feu (firewall), avec des règles de sécurité pour les flux entrants et sortants
Mises à jour du système et des logiciels
Sauvegarde : clé USB, disque dur externe, système RAID


sécurité informatique.pptx - LibreOffice Impress
Fichier Édition Affichage Insertion Format Diapo Diaporama Outils Fenêtre Aide
Diapos
Doctolib
AMeli.fr - Compte Profession
Site report for espacepro.am
https://toolbar.netcraft.com/site_report?url=espacepro.ameli.fr
Applications Bioserveur Agenda Réseau Sentinelles > ... Accueil Professionnels... bnp La Banque Postal HOMA Conseils aux Voyageu... Accueil sisra Consultation des Droits Bioserveur Autres favoris
Site report for espacepro.ameli.fr
Search...
Netcraft Extension
Home
Download Now!
Report a Phish
Site Report
Top Reporters
Incentives for reporters
Phishiest TLDs
Phishiest Countries
Phishiest Hosters
Phishiest Certificate Authorities
Phishing Map
Takedown Map
Most Popular Websites
Branded Extensions
Tell a Friend
Phishing & Fraud
Phishing Site Feed
Hosting Phishing Alerts
SSL CA Phishing Alerts
Protection for TLDs against Phishing and Malware
Deceptive Domain Score
Bank Fraud Detection
Phishing Site Countermeasures
Extension Support
FAQ
Glossary
Contact Us
Report a Bug
Tutorials
Installing the Extension
Using the Extension
Getting the Most
Reporting a Phish
Lookup another URL:
Enter a URL here
Share:
Background
Site title Not Present
Date first seen Not Present
Site rank
Primary language English
Description Not Present
Keywords Not Present
Netcraft Risk Rating [FAQ] 0/10
Network
Site http://espacepro.ameli.fr
Netblock Owner National Site CEN
Domain ameli.fr
Nameserver ns1.ascio.net
IP address 93.174.145.85 (VirusTotal)
DNS admin hostmaster@cscdns.net
IPv6 address Not Present
Reverse DNS espacepro.ameli.fr
Domain registrar nic.fr
Nameserver organisation whois.corporatedomains.com
Organisation caisse nationale de l'assurance maladie des travailleurs salaries, 26-50, avenue du Professeur Andre Lemierre, 75986 Paris, FR
Hosting company Corporation Service Company
Top Level Domain France (.fr)
DNS Security Extensions unknown
Hosting country FR
Sender Policy Framework
A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see openspf.org.
Warning: It appears that this host does not have an SPF record. Setting up an SPF record helps prevent the delivery of forged emails from your domain.
DMARC
DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see dmarc.org.
This host does not have a DMARC record.
Web Trackers
Démarrer
FR
13:04


sécurité informatique.pptx - LibreOffice Impress
Fichier Édition Affichage Insertion Format Diapo Diaporama Outils Fenêtre Aide
Diapos
Doctolib
AMeli.fr - Compte Profession
Site report for sfr.fr
https://toolbar.netcraft.com/site_report?url=sfr.fr
Site report for sfr.fr
Search...
Netcraft Extension
Home
Download Now!
Report a Phish
Site Report
Top Reporters
Incentives for reporters
Phishiest TLDs
Phishiest Countries
Phishiest Hosters
Phishiest Certificate Authorities
Phishing Map
Takedown Map
Most Popular Websites
Branded Extensions
Tell a Friend
Phishing & Fraud
Phishing Site Feed
Hosting Phishing Alerts
SSL CA Phishing Alerts
Protection for TLDs against Phishing and Malware
Deceptive Domain Score
Bank Fraud Detection
Phishing Site Countermeasures
Extension Support
FAQ
Glossary
Contact Us
Report a Bug
Tutorials
Installing the Extension
Using the Extension
Getting the Most
Reporting a Phish
Lookup another URL:
Enter a URL here
Share:
Background
Site title
SFR | Téléphone, Forfait Mobile, Internet + Fibre, Sport, Play, Presse, News
Date first seen
June 1997
Site rank
53552
Primary language
French
Description
D\303\251couvrez les offres Mobile, TV, Internet et Fibre de SFR. Choisissez le forfait qui r\303\251pond \303\240 vos besoins et retrouvez aussi le meilleur des contenus SFR Sport, SFR Play, SFR Presse.
Keywords
Mobile, TV, Internet
Netcraft Risk Rating [FAQ]
0/10
Network
Site
http://sfr.fr
Netblock Owner
SFR GPRS NETWORK
Domain
sfr.fr
Nameserver
ns1pub.sfr.fr
IP address
80.125.163.172 (VirusTotal)
DNS admin
support@dns.sfr.net
IPv6 address
Not Present
Reverse DNS
unknown
Domain registrar
nic.fr
Nameserver organisation
whois.nic.fr
Organisation
SOCIETE FRANCAISE DU RADIOTELEPHONE - SFR, 1, square Bela Bartok, 75015 Paris, FR
Hosting company
Numericable-SFR
Top Level Domain
France (.fr)
DNS Security Extensions
unknown
Hosting country
FR
Hosting History
Netblock owner
IP address
OS
Web server
Last seen
Refresh
SFR GPRS NETWORK 80.125.163.172 F5 BIG-IP Apache 14-May-2019
SFR GPRS NETWORK 80.125.163.172 F5 BIG-IP Apache/2.2.13 Fedora 15-Jul-2012
SFR GPRS NETWORK 80.125.163.172 F5 BIG-IP Apache/2.2.13 Fedora 5-Sep-2011
SFR GPRS NETWORK 80.125.163.172 F5 BIG-IP Apache-Coyote/rtm-sfrfr1 24-May-2011
SFR GPRS NETWORK 80.125.163.172 F5 BIG-IP Apache/2.2.13 Fedora 10-Apr-2011
SFR GPRS NETWORK 80.125.163.172 F5 BIG-IP Apache/2.2.13 Fedora 26-Feb-2011
SFR GPRS NETWORK 80.125.163.172 F5 BIG-IP Apache/2.2.13 Fedora 3-Dec-2010
SFR GPRS NETWORK 80.125.163.172 F5 BIG-IP Apache/2.2.13 Fedora 23-Oct-2010
Démarrer
FR
13:05

Lookup another URL:

Enter a URL here

Background

Site title	Surgica logiciel cabinet médical premium accessible en ligne	**Date first seen**	August 2014
Site rank		**Primary language**	French
Description	Testez d\303\250s maintenant le logiciel m\303\251decin premium Surgica accessible en ligne, logiciel chirurgien, m\303\251decin sp\303\251cialiste. Il prend en charge les rendez-vous en ligne m\303\251decin, les rappels de rdv par SMS et est accessible sur tous vos appareils Mac ou PC		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://surgica.fr	**Netblock Owner**	WSB HOSTING
Domain	surgica.fr	**Nameserver**	dns108.ovh.net
IP address	178.33.6.78 (VirusTotal)	**DNS admin**	tech@ovh.net
IPv6 address	*Not Present*	**Reverse DNS**	wp.wsb-agency.com
Domain registrar	nic.fr	**Nameserver organisation**	whois.ovh.com
Organisation	Medialog, Medialog, 9, rue laplace, 33700 MERIGNAC, FR	**Hosting company**	OVH
Top Level Domain	France (.fr)	**DNS Security Extensions**	*unknown*
Hosting country	FR		

Lookup another URL:

Enter a URL here

Share:

Background

Site title	Web hosting, cloud computing and dedicated servers- OVH	**Date first seen**	July 1997
Site rank	52014	**Primary language**	English
Description	OVH provides everything you need for a successful online project: web hosting, domain names, dedicated servers, CDN, cloud environments, Big Data...		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://ovh.com	**Netblock Owner**	OVH Hosting, Inc.
Domain	ovh.com	**Nameserver**	dns.ovh.net
IP address	198.27.92.1 (VirusTotal)	**DNS admin**	tech@ovh.net
IPv6 address	*Not Present*	**Reverse DNS**	www.ovh.com
Domain registrar	ovh.com	**Nameserver organisation**	whois.ovh.com
Organisation	OVH SAS, France	**Hosting company**	OVH
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	CA		

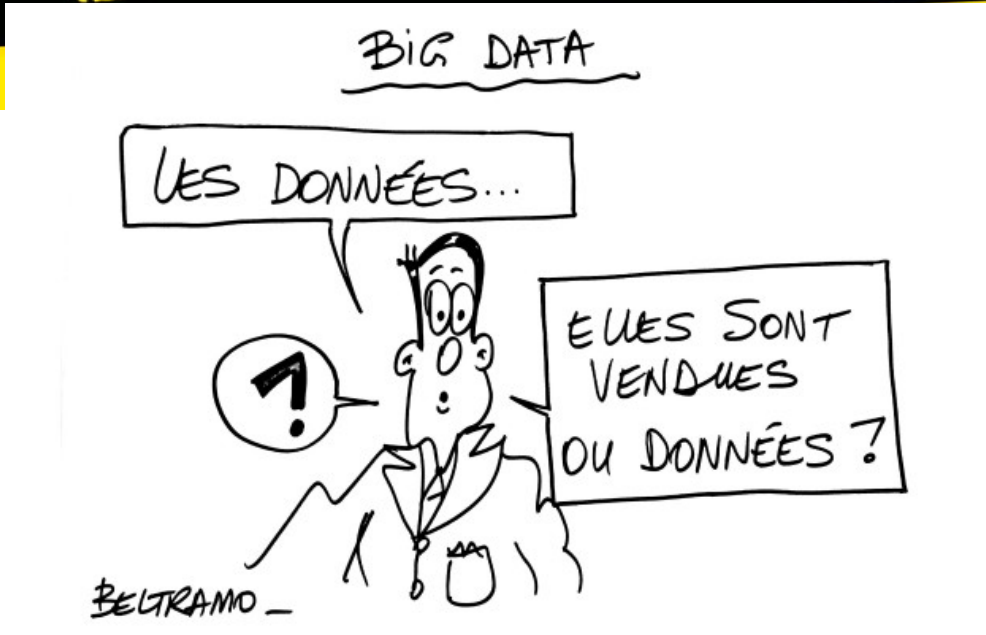
Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
OVH Hosting, Inc. 800-1801 McGill College Montreal QC CA H3A 2N4	198.27.92.1	Cisco	unknown	17-Mar-2019
OVH	213.186.33.34	Cisco	Apache	12-Feb-2017
OVH	213.186.33.34	unknown	Apache	5-Jan-2016
OVH	213.186.33.34	Cisco	Apache	21-Nov-2015
OVH	213.186.33.34	unknown	Apache	7-Nov-2015

Les objets connectés : Big Data / Big Brother

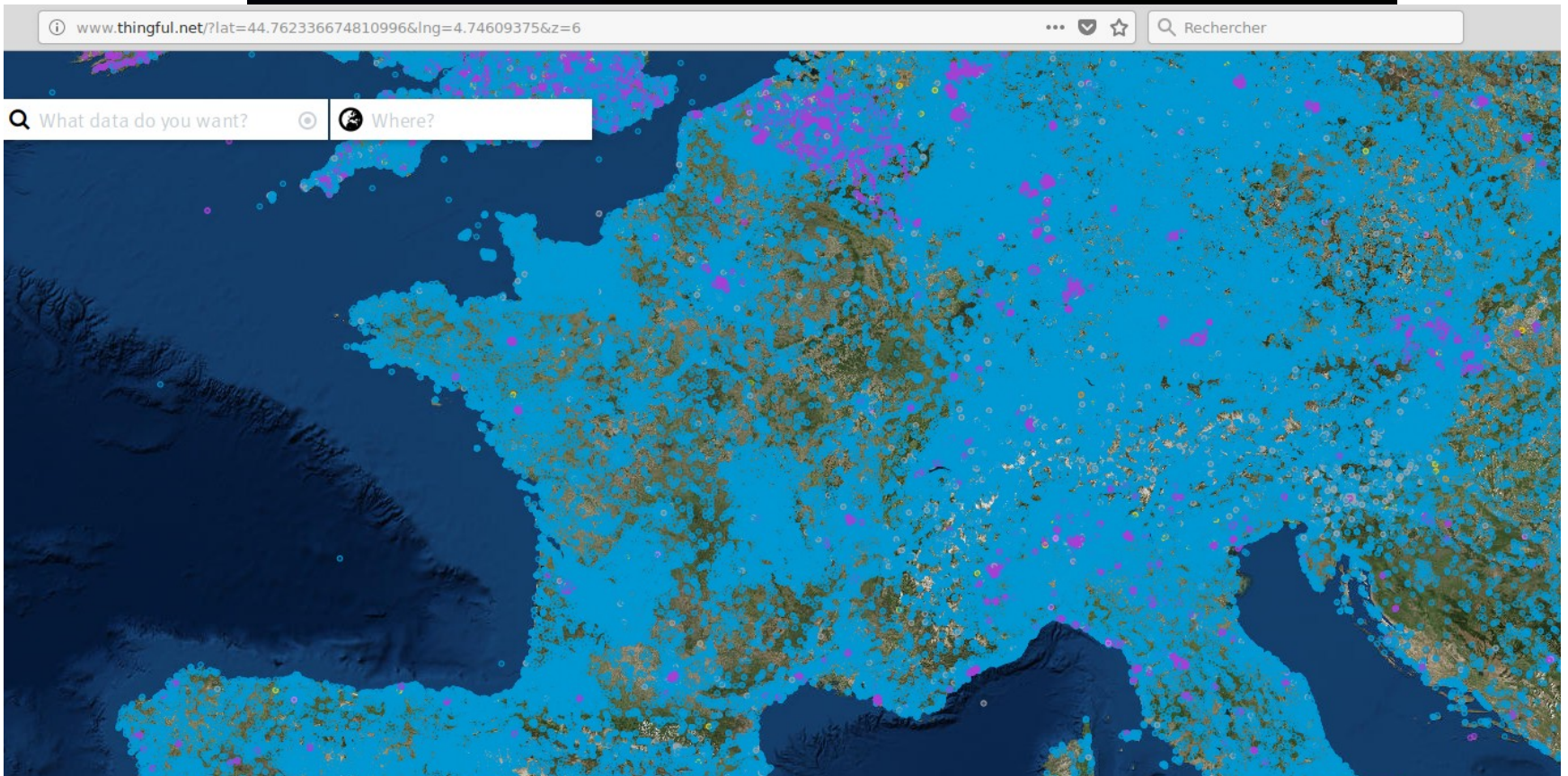
Les objets connectés : Big Data / Big Brother

LES NULS

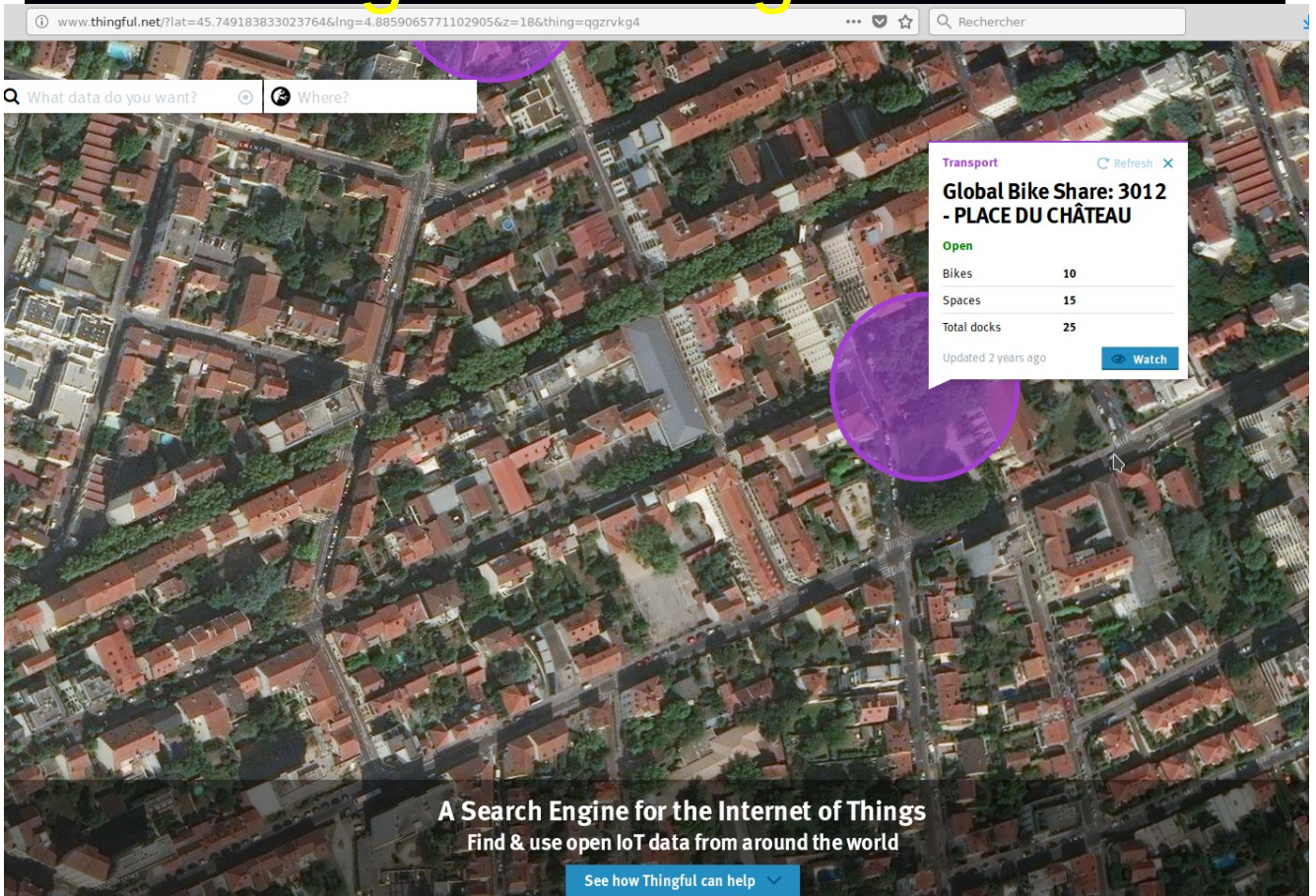


Vol de données
Partage sur les réseaux sociaux
Prise de contrôle à distance (pace maker)
Géolocalisation
Modification des informations
Introduction de virus, pannes….

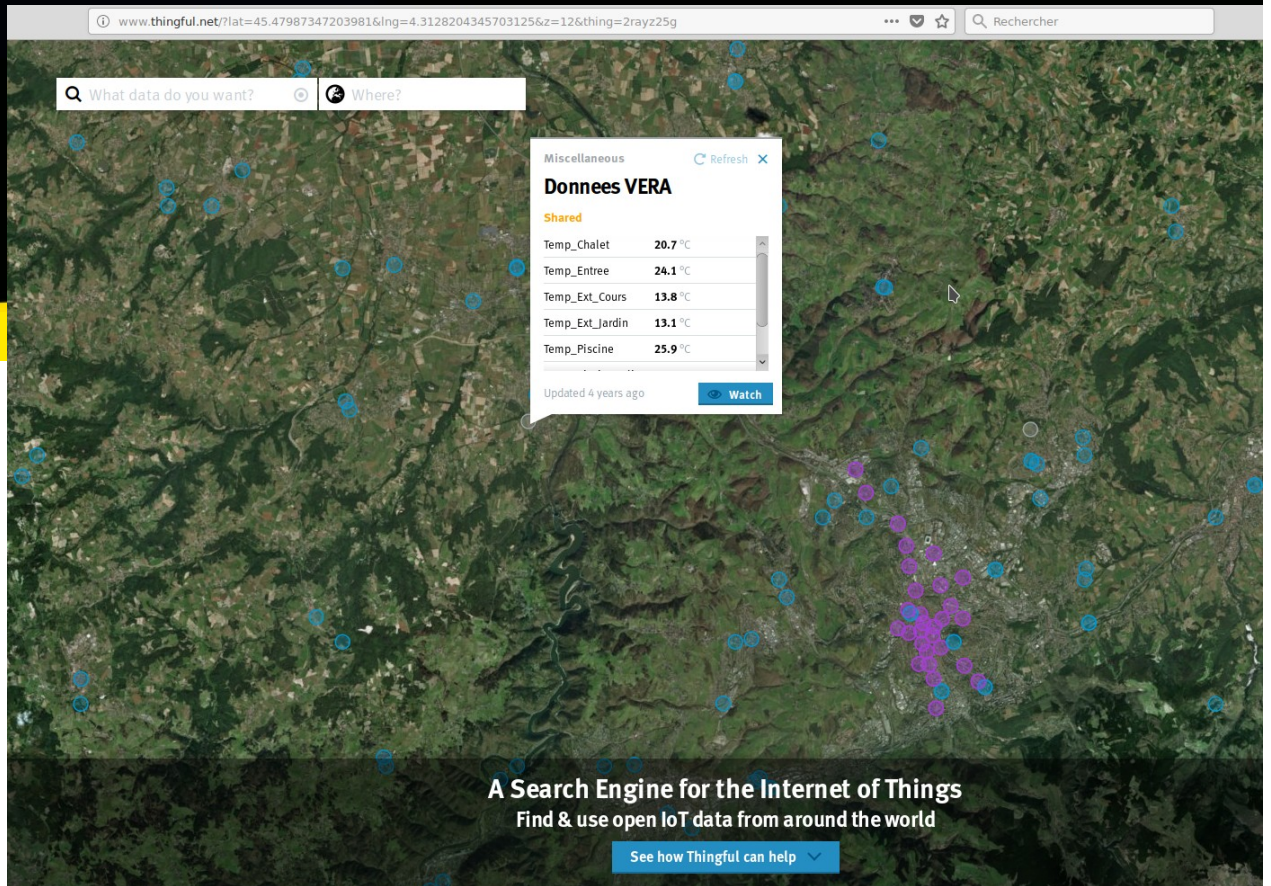
Les objets connectés :
Big Data / Big Brother



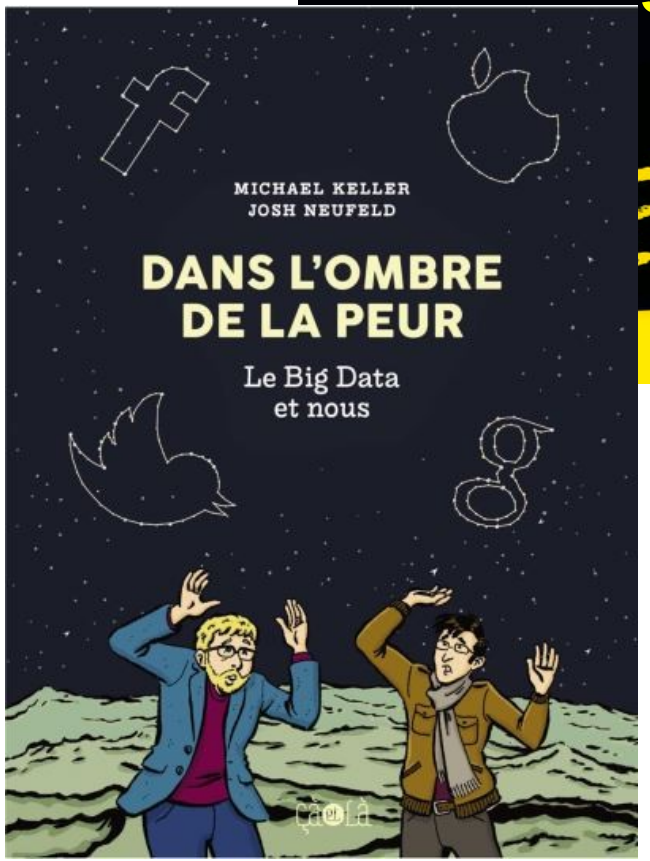
Les objets connectés : Big Data / Big Brother

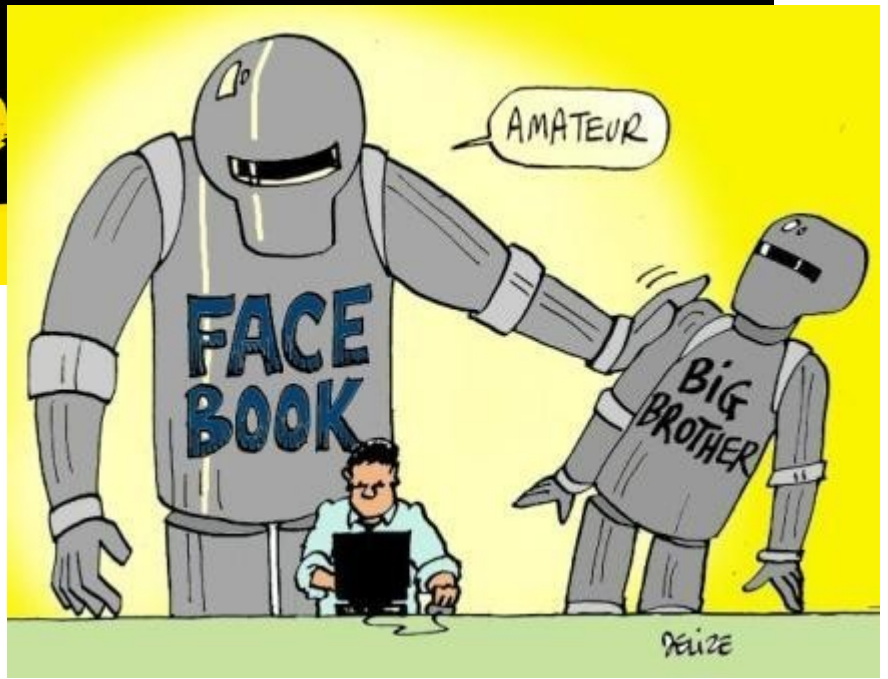


Les objets connectés :
Big Data / Big Brother



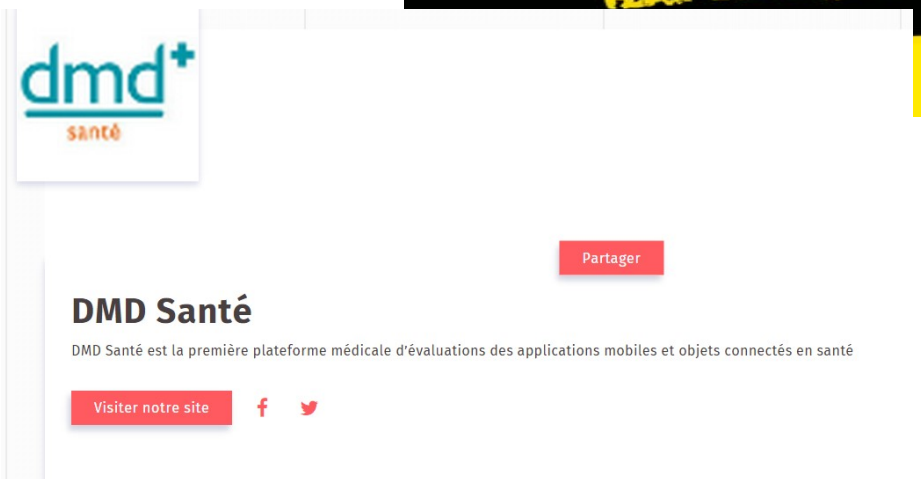
Les objets connectés : Big Data / Big Brother

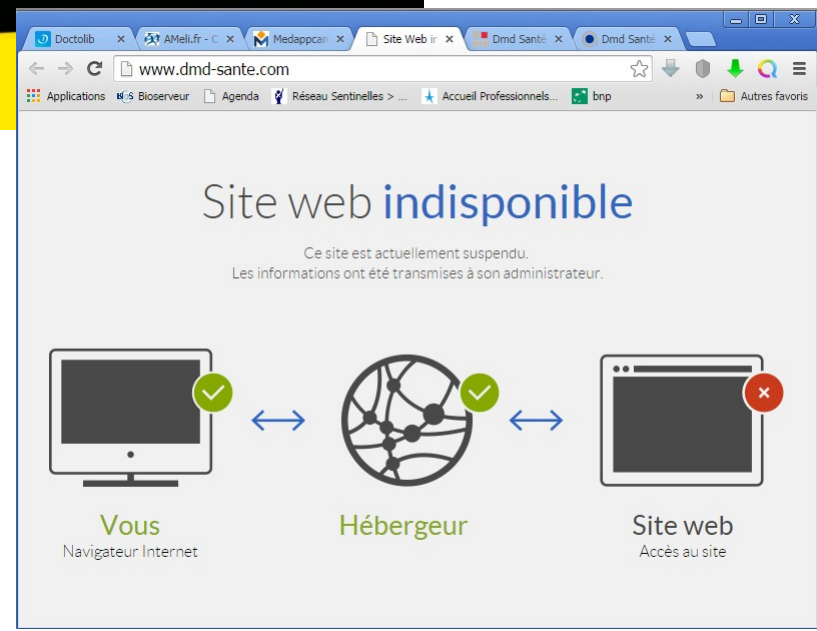




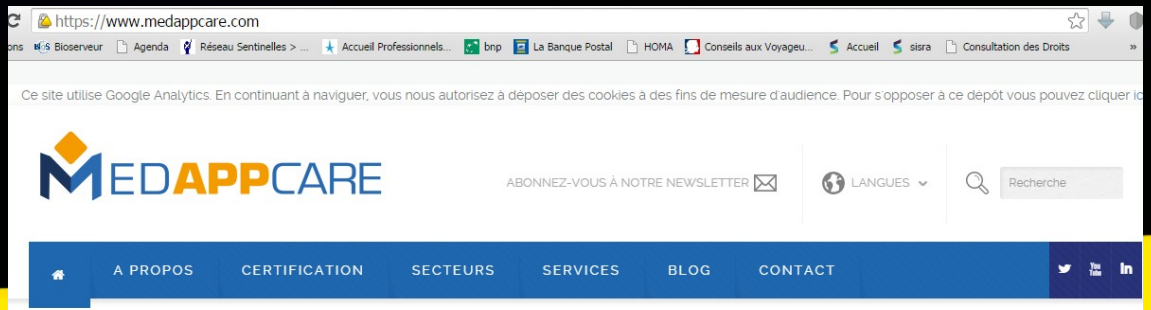
Les objets connectés : Big Data / Big Brother

LES NULS





Les objets connectés : Big Data / Big Brother

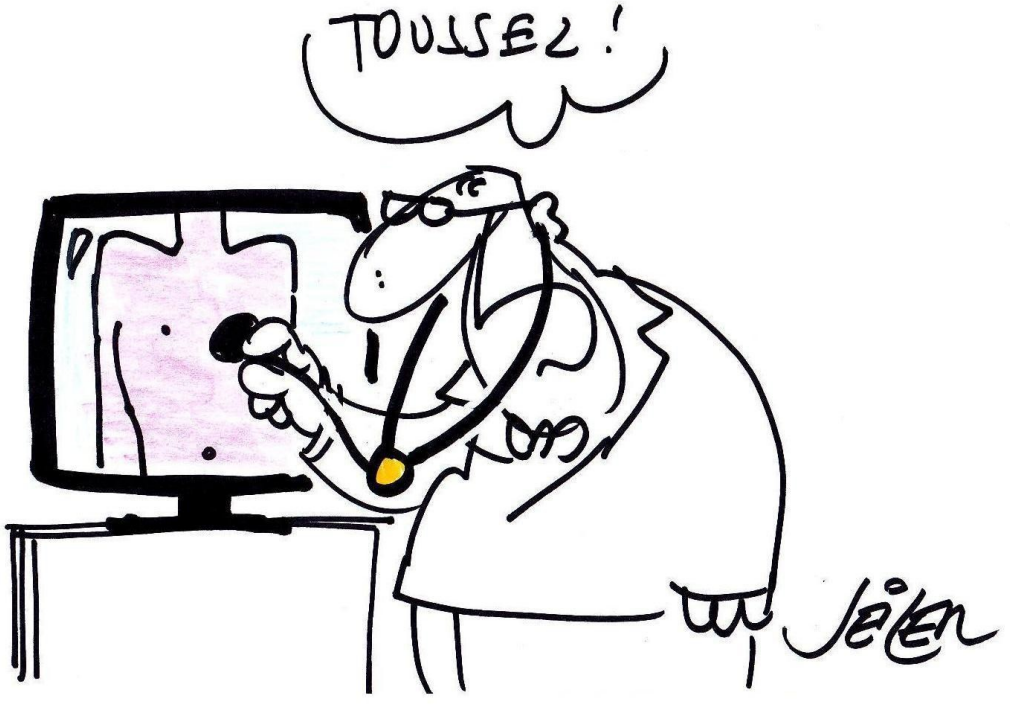


Notre métier

Le parcours de vie des individus est optimisé par de nombreux services web et mobiles prometteurs en terme de santé, d'autonomie et d'accessibilité, mais la qualité de ces services n'est pas toujours au rendez-vous. Medappcare est l'organisme certificateur du mieux-vivre

L’Intelligence Artificielle par

La télémédecine
Par



Échanges et questions

Contactez Sébastien CLAUDE
06 47 74 82 11
Sebastien.claude@asc2si.fr

ASC2SI
LA RÉSILIENCE DE VOTRE SYSTÈME