Réf : N° PAN/216/085/PSI
jeudi 18 août 2016
Version 3

HOSEN
Rapport de valorisation

Soutenir la recherche
pour prévenir les risques

L'OBJECTIF DE CE DOCUMENT EST D'EXPOSER
LES RESULTATS DES TRAVAUX DU PROJET HOSEN (HOME SECURITY NETWORKS)
SOUTENU PAR LA FONDATION MAIF

Panga

TABLE DES MATIERES

1. PREAMBULE

1.1 Interlocuteur

Pour toutes questions relatives à ce document, vous pouvez prendre contact avec la personne suivante qui a contribué à son élaboration :

- **Patrick SIMON**

patrick.simon@panga.fr
06.19.67.00.6
1 rue Fleming, 17000 LA ROCHELLE

1.2 Avertissement

Si ce document est d'un indice supérieur à ceux diffusés ou transmis, il les annule et les remplace.
En conséquence, son destinataire doit, dès réception :

1. Détruire les versions antérieures après vérification des changements précisés ci-dessus.
2. Remplacer les documents détruits par le présent document.
3. Appliquer cette règle (destruction/remplacement) à l'ensemble des documents copiés sous sa responsabilité avec l'autorisation écrite de PANGA.
4. S'assurer, en cas d'obligation de conservation, que les versions antérieures ne peuvent être utilisées (la dernière version faisant foi).

2. INTRODUCTION

Ce document est le rapport de valorisation des travaux qui ont été menés par l'entreprise PANGA dans le cadre du développement du Projet HOSEN (HOme Security Networks).
Ce projet a pour objectif de sécuriser les données personnelles issues des objets connectés.
Ce projet a bénéficié d'un financement de la Fondation MAIF.

Dans le cadre des travaux menés, divers livrables et documents ont été fournis.

- **Livrable A**
  Etat de l'art, définition des cas d'usage
  Document référence IOT215024JDA_V3_Etude_prealable_et_etudes_de_cas
  Document référence IOT215059FMI_V2_Complement_Etude_prealable_et_etudes_de_cas

- **Livrable B**
  Prototype d'une plateforme matérielle assurant la connexion et le support des différents équipements et objets connectés au domicile
  Document référence PAN215000FMI_V5_Spécifications_matérielles

- **Livrable C**
  Traitement des données issues du Prototype de la plateforme matérielle

- **Livrable D**
  Développement des fonctions de sécurisation

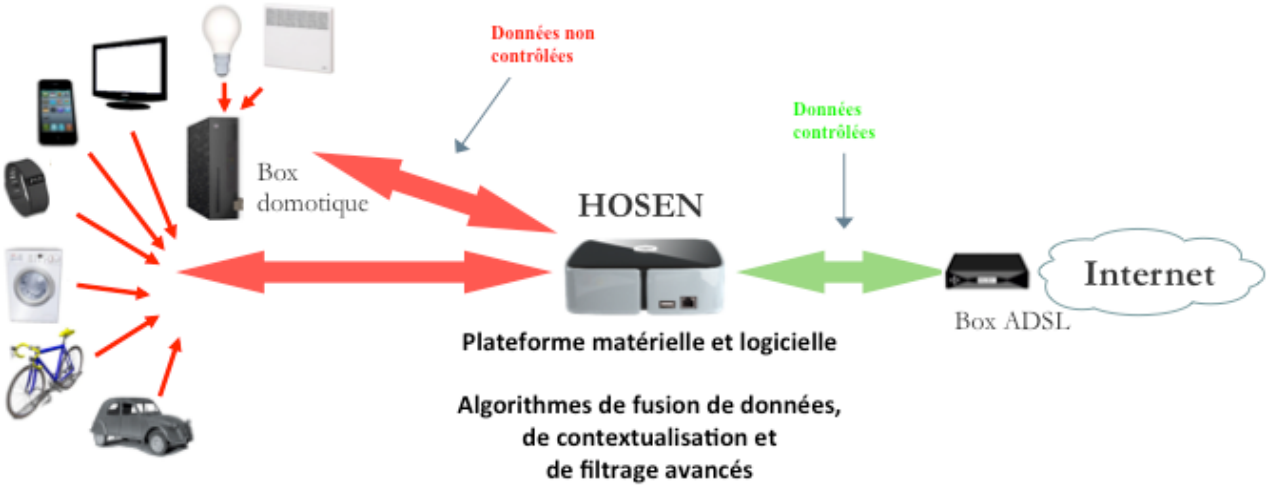
- **Livrable E**
  Mise en œuvre du prototype

- **Livrable F**
  Rapport de synthèse
  Document référence PAN215002JDA_V3_Hosen – Synthèse scientifique
  Rapport de valorisation (ce document, référence PAN216085PSI)

3. RAPPEL DES OBJECTIFS DU PROJET HOSEN

Le Projet Hosen vise la conception et le développement d'une solution prototype permettant d'assurer la fédération et la sécurisation des données personnelles issues des objets connectés de l'habitat.
Il s'appuie sur l'utilisation de composants matériels informatiques embarqués et de composants logiciels intégrés au domicile. Il crée une structure permettant de fédérer les objets connectés actuels et à venir.

Illustration du concept



4. LES DONNEES PERSONNELLES

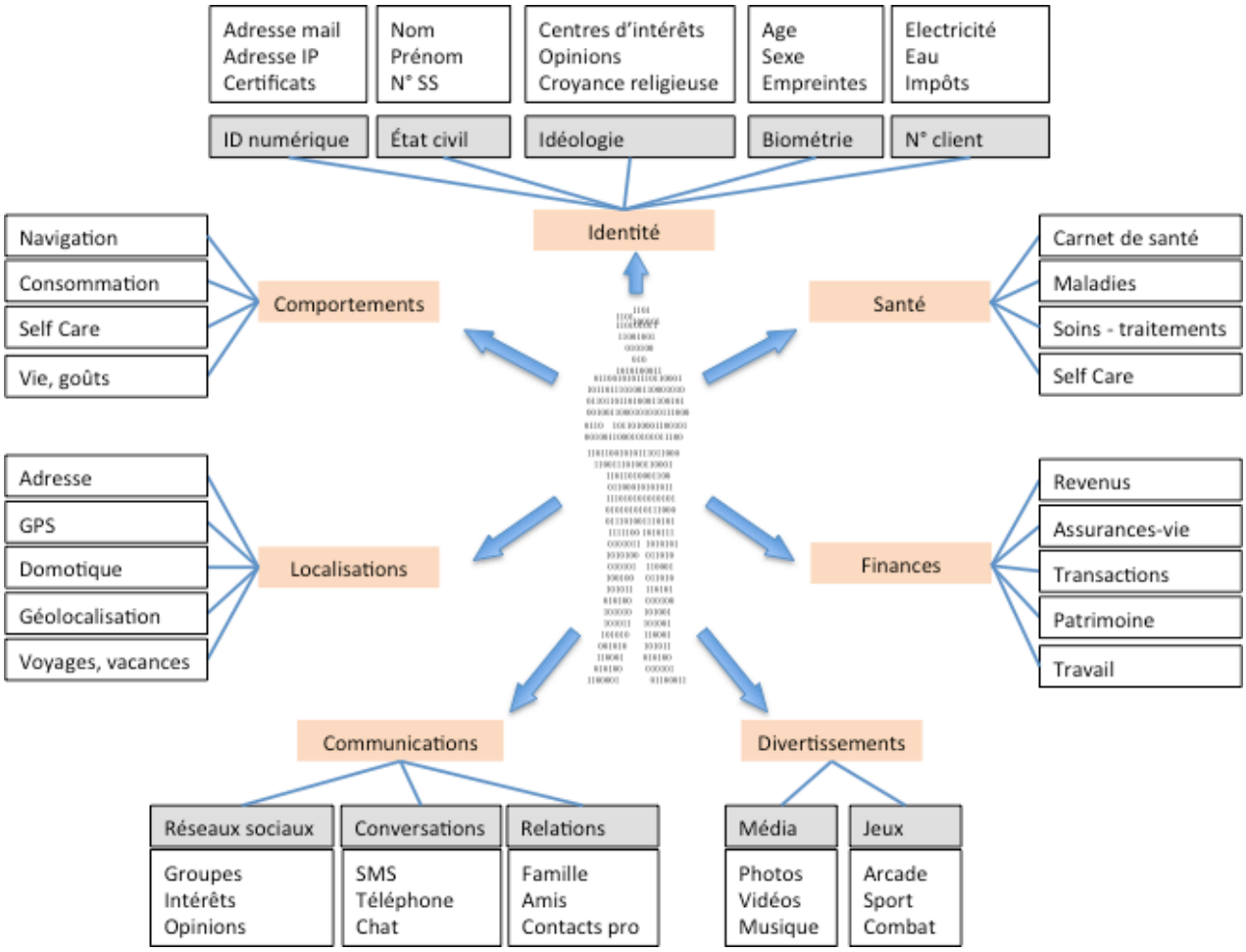
4.1 Définition

Une donnée personnelle est définie comme un ensemble d'informations qui permet d'identifier une personne :

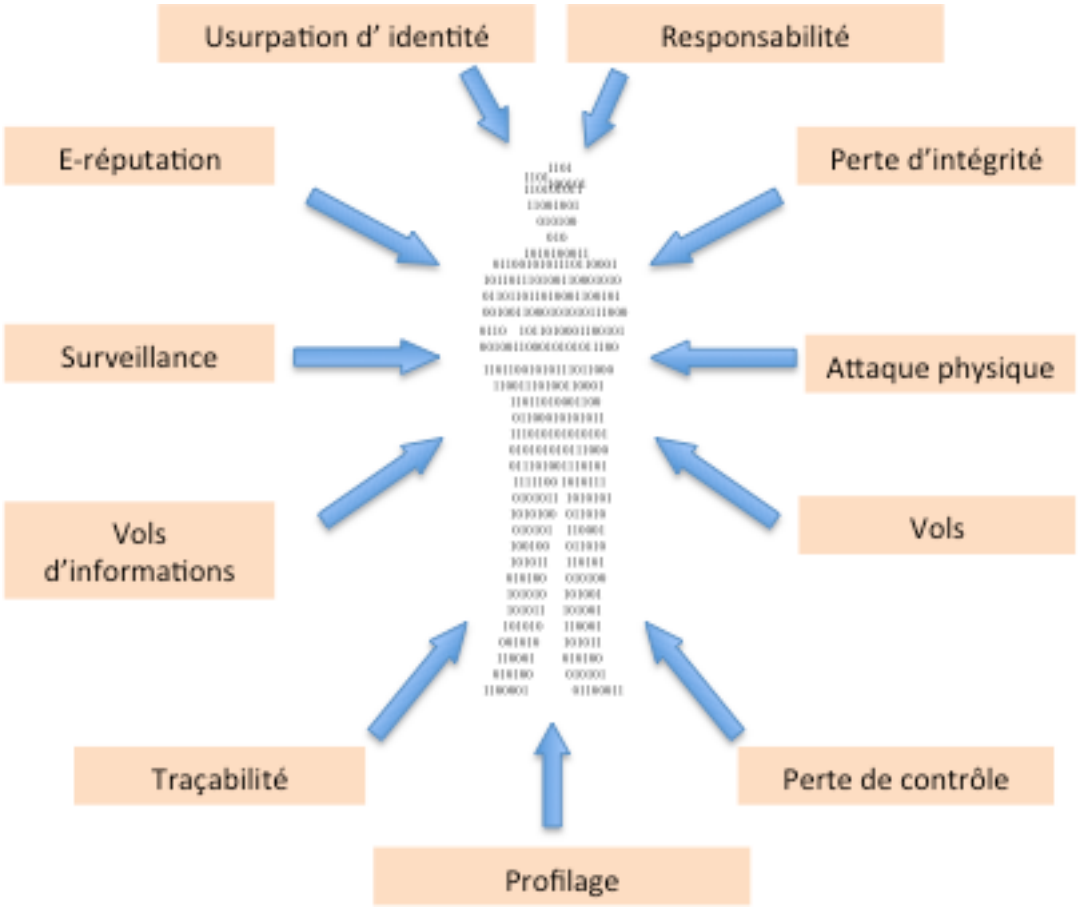
- directement
- ou indirectement (ex : numéro de Sécurité Sociale)
- ou par regroupement (ex : une date de naissance associée à une commune de résidence,

et de connaître de cette personne un certain nombre de caractéristiques (schéma ci-dessous).

Cette cartographie permet de regrouper l'ensemble des données personnelles qu'il est possible de récupérer via internet ou via les objets connectés.



4.2 Les risques potentiels



Dans le cadre de nos travaux, nous avons classifié les données personnelles (DP) en 6 catégories :

- DP1 - Je m'identifie en maîtrisant mes données
  (ex : formulaire administratif)
- DP2 - Je donne volontairement des données
  (ex : site de e-commerce)
- DP3 - On me prend mes données
  (ex : virus ou application douteuse sur un smartphone)
- DP4 - Un de mes proches donne à ma place des données
  (ex : publication sur un réseau social)
- DP5 - Un objet donne des données
  (ex : pèse personne qui envoie mon poids et son évolution sur un site externe)
- DP6 - On m'a calculé
  (ex : des tiers vendent mes données à d'autres qui les agrègent)

4.3 Constat

D'ici à 2020, le monde pourrait comporter 10 milliards d'habitants, dont 5 milliards d'internautes.
Il y aurait 10 milliards de nouvelles connexions de machine à machine, et une multiplication par onze du trafic des données entre mobiles.

Il est alors primordial que les gens prennent conscience de l'importance de la sécurité de leurs informations sur internet, beaucoup plus vulnérables que le matériel d'un simple ordinateur. Ces données mobiles deviennent monnayables, c'est-à-dire avec une valeur économique, qui peut faire l'objet de transactions économiques.
Les objets connectés transmettent des données qui peuvent être récupérées par un tiers pour être revendues. L'utilisation de ces données génère aussi des risques :

- perte de réputation
- vol d'informations
- atteinte à la vie privée
- traçabilité de la vie.

4.4 Quelques exemples de communication

La numérisation du monde est en marche. La donnée est devenue une valeur marchande où nous sommes tous producteurs et acteurs
Mais qu'en est-il de la sécurité des données associées aux technologies numériques ?

On commence à en parler :

L'ARGUS DE L'ASSURANCE du 12 décembre 2014 N° 7389 fait état des préoccupations des principaux groupes d'assurance au regard des données personnelles.

LA TRIBUNE a également publié un article sur le sujet :
http://www.latribune.fr/opinions/tribunes/20140618trib000835759/objets-connectes-attention-a-l-espionnage-domestique.html
Un article des plus complets sur le sujet avec le point de vue d'analystes, de juristes et de la CNIL :
http://www.lesnumeriques.com/objets-connectes-securite-donnees-a1790.html

Une étude du CSA mandaté par le groupe ORANGE a également été réalisée auprès des français sur ce sujet :
http://www.csa.eu/multimedia/data/sondages/data2014/opi20140123-les-francais-et-la-protection-des-donnees-personnelles.pdf

Le PARLEMENT EUROPEEN a lui aussi publié un Guide de protection des données personnelles à destination des parlementaires européens et de toutes personnes travaillant dans ce périmètre :
http://www.europarl.europa.eu/pdf/data_protection/guide_fr.pdf

TF1 a également évoqué le sujet lors du Journal télévisé du jeudi 20 février 2014 à 20h35 :
http://videos.tf1.fr/jt-20h/2014/attention-aux-objets-connectes-nouvelle-cible-des-pirates-informatiques-8369610.html

Un reportage sur ARTE du 24 mars 2015 (Un œil sur vous) d'une heure et demie sur l'espionnage des données personnelles, les mouvements contestataires, et un aperçu d'un projet européen visant à sécuriser les données personnelles.

Chiffres d'utilisation du NET
http://www.blogdumoderateur.com/chiffres-internet/

Article de la CNIL autour des IOT
https://www.cnil.fr/fr/internet-sweep-day-2016-comment-les-objets-connectes-du-quotidien-impactent-la-vie-privee

L'ARGUS DE L'ASSURANCE à nouveau
http://www.argusdelassurance.com/acteurs/big-data-protection-des-donnees-personnelles-attention-danger.103701

Etude de marché sur les données personnelles
http://www.expertinbox.com/partage-de-donnees-personnelles/

5. PRINCIPALES CONCLUSIONS

5.1 Une demande qui augmente

Suite aux révélations d'Edward Snowden et l'affaire PRISM à propos de la surveillance électronique massive de la NSA à travers un système auquel personne n'échappe, la sécurité des données personnelles apparait comme un problème majeur pour la plus grande partie de la population.

Quatre grandes entreprises américaines se sont rapidement développées grâce à l'analyse des données personnelles : Google, Apple, Facebook et Amazon. A noter que pas un seul groupe européen ne rivalise avec eux.
Maîtriser ses données personnelles est donc dès aujourd'hui un vrai défi.

Aujourd'hui, les entreprises qui captent les données massives des utilisateurs individuels en tirent plusieurs centaines de milliards de dollars de chiffre d'affaires. Selon les estimations du Data-Driven Marketing Institute, ce secteur du « data mining » aurait créé quelque 156 milliards de dollars (1 220 milliards d'euros) de chiffre d'affaires en 2012, soit près de 60 dollars pour chacun des 2,5 milliards d'internautes dans le monde …
La valeur totale des données personnelles des citoyens européens représenterait ainsi 330 milliards d'euros par an pour les organisations publiques et privées. Pour les entreprises européennes dont le métier fait appel aux données personnelles, on estime que cela représente une croissance de 22% des bénéfices . Les secteurs d'activité se basant sur la gestion de l'identité numérique peuvent prétendre à des taux de croissance annuels entre 15% et 100%.
La libéralisation de l'usage de ces données représenterait un gain potentiel de 670 milliards d'euros par an pour les entreprises qui récupèrent les données.

5.2 Prise de conscience

La prise de conscience des usagers est encore faible. Lorsque l'on interroge les habitants de différents pays à travers le monde sur la sécurité des données personnelles (enquête IPSOS), on se rend compte que les français ne sont pas encore très concernés par la question.

En effet, la moyenne mondiale du nombre de personnes très concernées par la sécurité des données personnelles est de 31% alors qu'elle n'est que de 20% à l'échelle de la France. Cependant, la tendance des personnes un peu concernées par la question a tendance à suivre la moyenne mondiale.

Alors que faire ?

5.3 Préconisations

5.3.1 Profil des usagers

Plusieurs études ont été réalisées afin de définir plusieurs profils d'utilisateurs face à la problématique de la protection des données personnelles, dont l'étude HAVAS MEDIA "Les français et les données personnelles", octobre 2014.
L'étude a pris en compte plus de 1000 internautes de 15 à 64 ans, représentatifs de la population française. La typologie suivante a ainsi été mise en valeur :

- **Les Data Paranos – 36%**
  Population plus âgée (plus de 35 ans, dont les 50/64 ans), consciente et très inquiète.
  Ils ne comprennent pas à quoi peuvent servir leurs données personnelles. Ils ont peur de l'utilisation frauduleuse de leurs données, et se protègent comme ils le peuvent.
- **Les Data fatalistes -27%**
  Population assez jeune et fataliste.
  Ils comprennent que leurs données sont récupérées mais se protègent peu. Cible féminine et CSP -.
- **Les Data Natives – 24%**
  Population jeune (15 à 34 ans) et peu inquiète de l'utilisation de leurs données.
  La récupération et la transmission des données personnelles est une chose normale et habituelle.
- **Les Data Stratèges – 9%**
  Population plus âgée (35 à 49 ans), masculine, parisienne, CSP + et pour moitié avec enfants
  Conscients de ce que valent leurs données, ils cherchent à obtenir des contreparties.
- **Les Data Détendus – 4%**
  Population peu consciente du phénomène lié aux données personnelles.
  Est donc peu inquiète.

Toute communication devra être adaptée selon les populations ciblées.

5.3.2 Les attentes des usagers

- 36% des européens et 37% des français jugent que c'est à l'État d'agir, avec plus de sévérité et d'efficacité.
- 30% des européens et 36% des français jugent que c'est avant tout aux entreprises d'œuvrer pour que les données soient mieux protégées.
- 33% des européens mais seulement 27% des français estiment que c'est de la responsabilité des individus eux-mêmes.

5.3.3 Pistes d'amélioration et gestion de la prévention

La donnée personnelle présente un risque, mais c'est un risque immatériel, qui est donc difficilement perceptible par les usagers.

Différents moyens devront être déployés afin de sensibiliser les usagers.

Une approche indirecte

- Promouvoir une campagne d'information à grande échelle destinée à sensibiliser les citoyens aux enjeux liés à la vie privée et à la protection des données personnelles ;
- Vulgariser l'information relative à la sécurité informatique ;
- Promouvoir une campagne d'information à grande échelle destinée à sensibiliser les citoyens aux enjeux sur les risques liés à l'usage d'internet ;
- Compléter, étendre et adapter le cadre juridique aux nouvelles technologies ;
- Renforcer la place accordée à la sensibilisation sur la loi "Informatique et Liberté" du 6 janvier 1978 et sur le droit à l'oubli ;
- Informer le citoyen de manière claire, précise et concise sur les données à caractère personnel enregistrées, utilisées ou vendues à des tiers par les organisations privées (et publiques), ou même les individus.

5.3.3.1 Une approche directe

S'appuyer sur les réseaux de conseil aux usagers pour les sensibiliser, tels que les banques, les assureurs, les fournisseurs d'énergies, les agents de La Poste, etc.

Avec l'accélération du numérique et l'accès facilité - par les révolutions technologiques - des collecte, consultation et exploitation des données individuelles et personnelles, de nouveaux acteurs appréhendent avec une granularité fine les besoins des clients et peuvent proposer des produits autrefois réservés aux spécialistes de l'assurance.

La connaissance des individus s'accélère avec la numérisation et les outils de traçabilité liés à l'introduction du numérique dans tout les objets du quotidien. Ainsi les grands de l'internet connaissent parfois mieux le comportement des usagers, et savent mieux analyser leurs situations face aux risques, que les assureurs eux-mêmes.

5.3.4 Les acteurs les mieux placés

La donnée est une richesse. Elle présente également des risques pour l'individu, pour la collectivité, voire pour la nation.
L'assureur doit jouer son rôle de gestion et de prévention des risques ; la donnée personnelle doit être prise en compte au même titre que l'habitation ou la voiture.

L'assurance est en effet au cœur de la société et en interaction avec toutes les activités. Pour protéger les acteurs contre les risques qu'ils encourent, l'assurance doit connaitre intimement ces activités : leurs spécificités, leurs besoins, leurs développements, et les innovations.

L'anticipation de l'évolution des risques existants, et la connaissance des risques émergents sont indispensables à une activité d'assurance pérenne, d'autant que les assureurs prennent souvent des engagements de long terme auprès de leurs sociétaires et assurés.

Il faut repousser sans cesse la frontière de l'assurabilité par l'innovation, en associant à des contrats classiques MRH (multirisque habitation) des solutions de prévention liées à la gestion des données personnelles.

5.3.5 Actions selon les domaines d'activité stratégique et d'innovation prioritaire

DAS /IP 1
Former les équipes des réseaux de commercialisation
aux nouveaux métiers de prévention des risques, et aux conseils personnalisés liées aux données personnelles.

DAS /IP 2
Participer au développement d'outils d'expertise et de conseil pour les commerciaux.

DAS /IP 3
Participer au développement d'outils de communication auprès des assurés et sociétaires
(films / animations / campagne de communication, …).

DAS /IP 4
Développer de nouveaux services et contrats associés à ces nouveaux risques
en conservant la confiance de l'assuré et/ou sociétaire.
(contrat MRH / RCP / RC qui prend en compte la protection et la gestion de l'e-réputation, et la perte d'exploitation liée).

DAS /IP 5
Simplifier les contrats et les outils par la mutualisation des risques

DAS /IP 6
Prendre en considération l'évolution du cadre législatif.