

Sécurité et identité(s) numérique(s)

Jessica EYNARD

Maître de conférences HDR en droit
Université Toulouse Capitole
Jessica.eynard@ut-capitole.fr



Giorgia MACIOTTI

Chercheur à l'IRIT, CNRS
Institut cybersécurité Occitanie
Giorgia.macilotti@irit.fr

Partenaires de plusieurs projets européens :

- ✓ Projet H2020 Legality Attentive Data Scientists (LeADS), H2020-MSCA-ITN-2020.
- ✓ Projet Horizon Europe Data Usage Control for empowering digital sovereignty for All citizens (DUCA)
- ✓ Projet EU Check



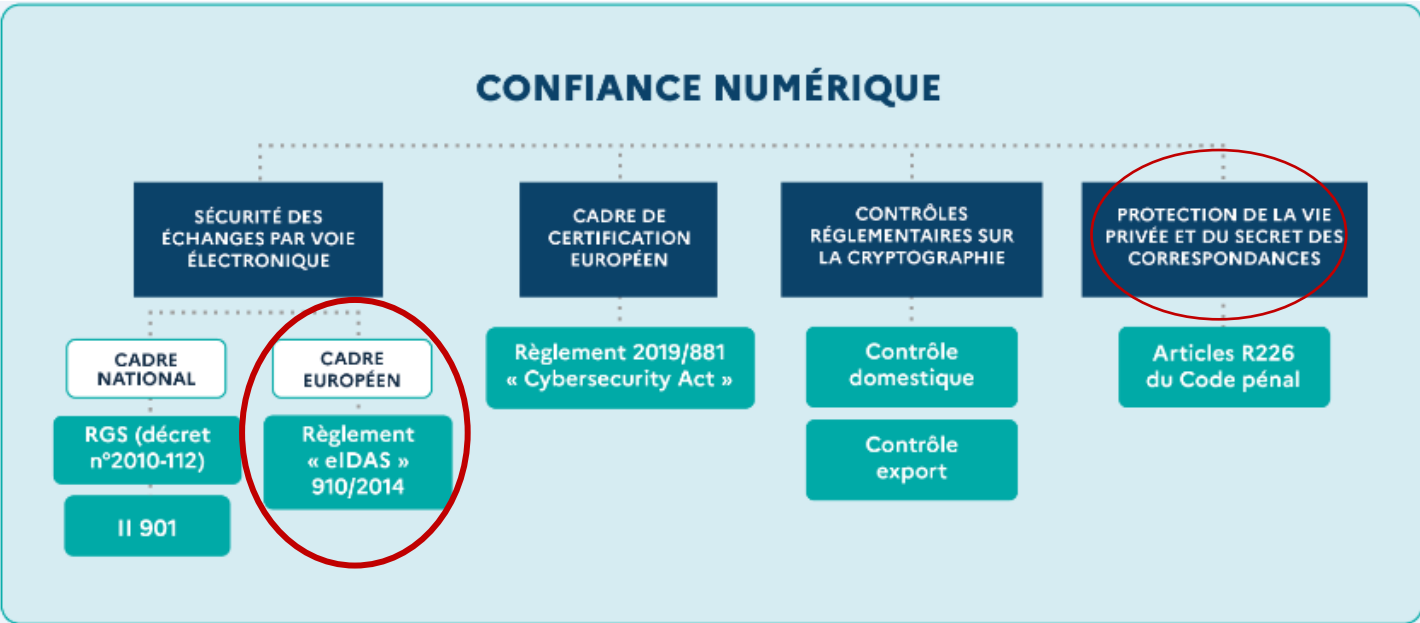
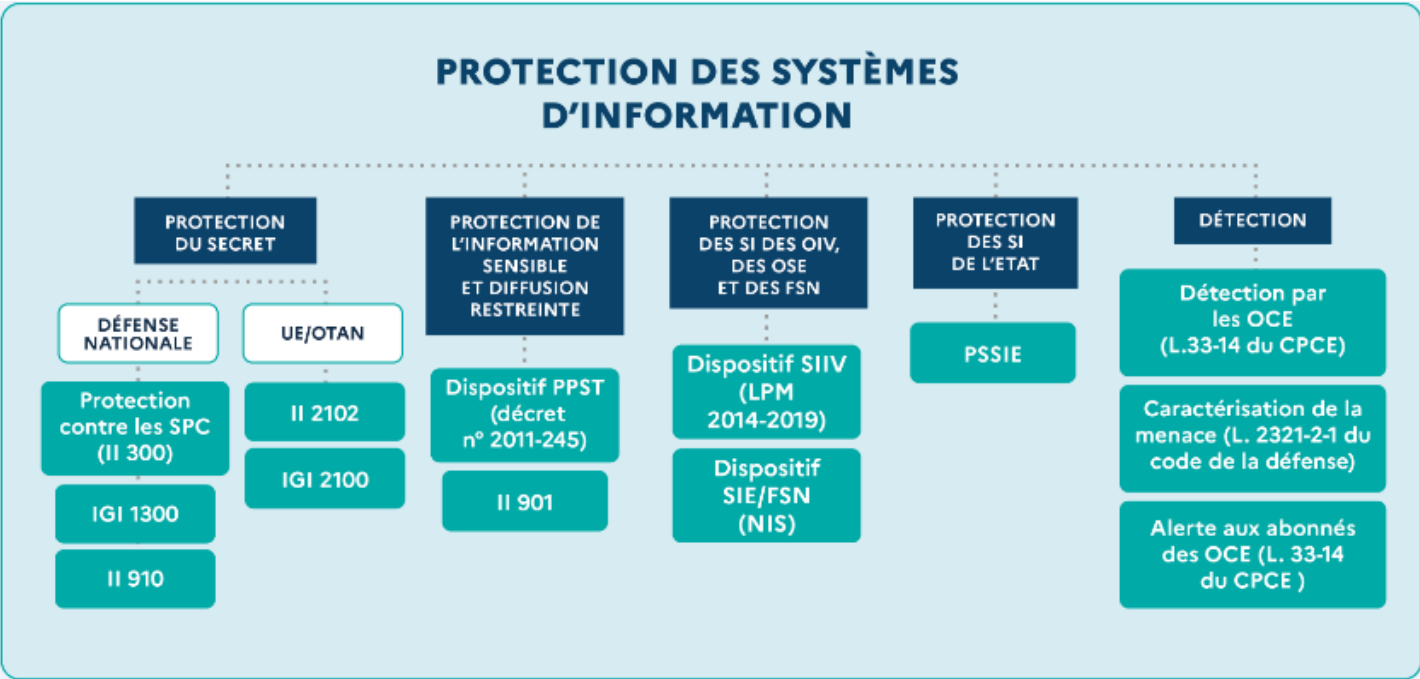
Lycée Ozenne
Toulouse



Lien sécurité/identité



Deux grandes catégories de textes « cyber »



Le contexte et les enjeux de l'étude



Conceptualisation(s) « **identité numérique auto-souveraine** »



Modes d'identification à distance présents et à construire

Enjeux et risques
pour les droits et
libertés
fondamentaux



Objectifs

- 1) juger de la capacité d'une personne à « gérer » les éléments de son identité en ligne
- 2) Sur cette base, faire des propositions pour une identification en ligne acceptable et respectueuse des droits et libertés fondamentaux

Approche méthodologique



4 ateliers de travail et
réunions mensuelles



Entretiens semi-directifs :

- ✓ professionnels (N : 8)
- ✓ étudiants BTS (N : 19, 18-21 ans)

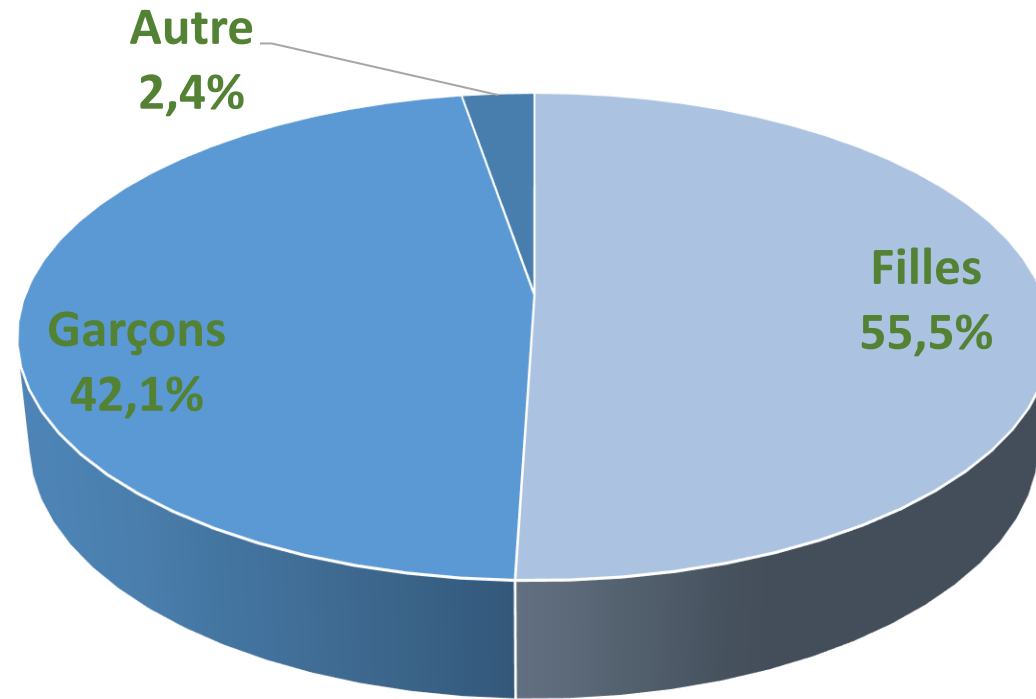


Focus group : étudiants
BTS (N : 12, 18-20 ans)

Enquête par questionnaire

- ✓ Construction instrument de mesure (avril-juin 2021)
- ✓ **Questionnaire validé** par le **CER** de l'université fédérale (septembre 2021)
- ✓ **Echantillonnage** (filière BTS, 17-22 ans) + collecte formulaires de consentement (septembre-octobre 2021)
- ✓ **Test du questionnaire** (octobre 2021, 17-19 ans, N : 22)
- ✓ Passation du questionnaire (novembre 2021 – février 2022) : **procédure auto-administrée** à l'ordinateur (Limesurvey)
- ✓ Analyse des données : **SPSS** et traitement lexicométrique des réponses ouvertes (classification descendante hiérarchique, **Iramuteq**)

Les répondants



371 étudiants - filière post-baccalauréat (BTS)

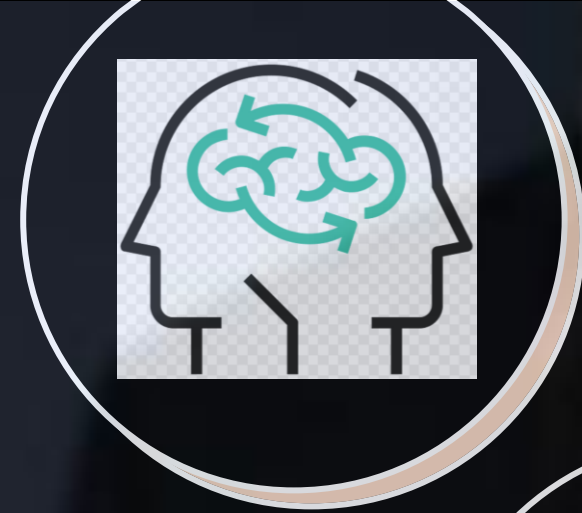
Âge : **17-22 ans** - âge moyen 19 ans



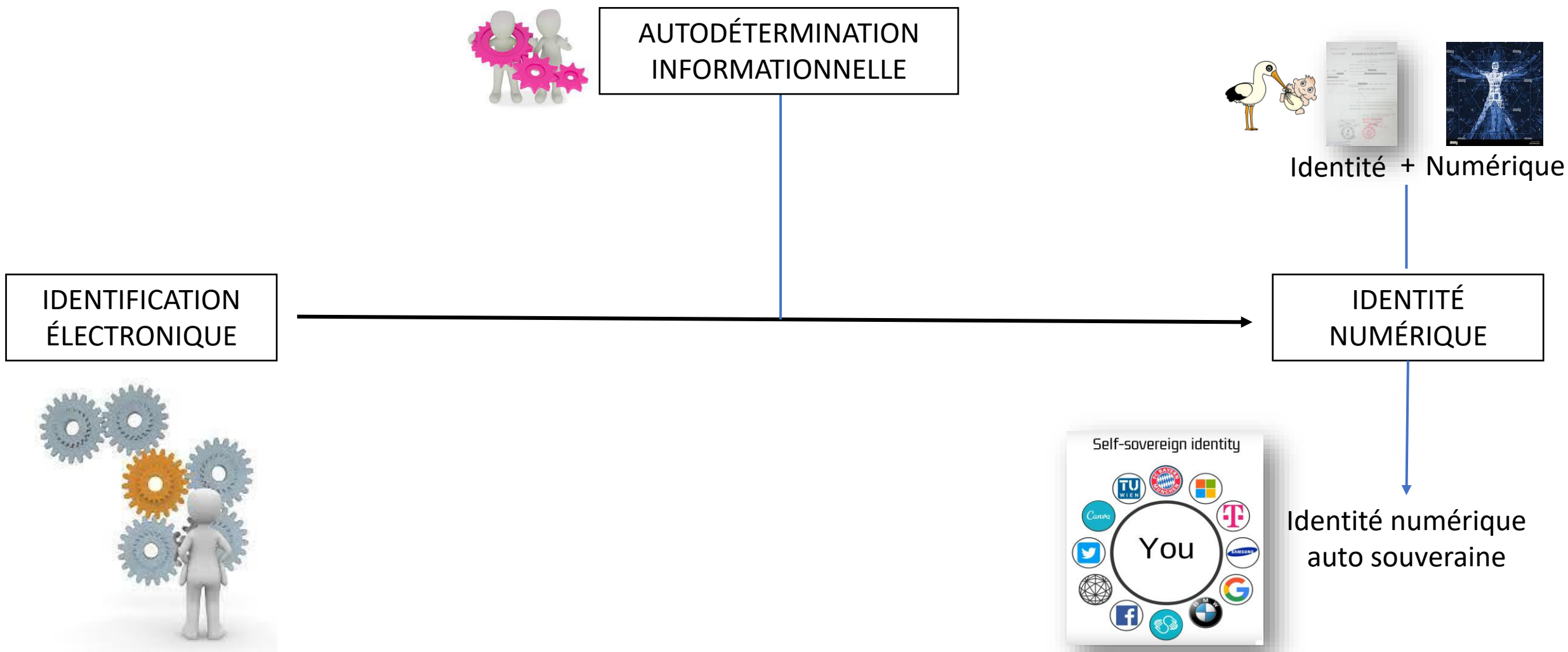
Partie 1

A la recherche d'une identité numérique auto-souveraine

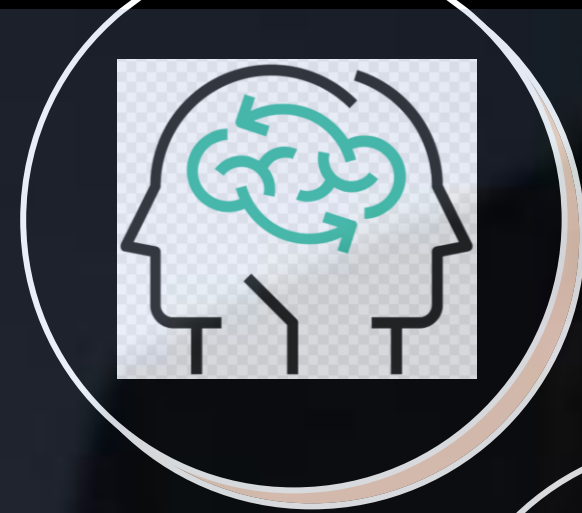
A la recherche d'une identité numérique en théorie



L'identité numérique en sciences sociales



A la recherche d'une identité numérique en pratique



L'identité numérique pour les répondants

Image performée, stratégique

« C'est l'image qu'on montre sur internet » ;
« ce que les gens choisissent de montrer sur leurs réseaux sociaux ... »

Distance identité « réelle » et numérique

« Une identité numérique n'est pas forcément la même qu'une identité dans la vie réelle. Sur Internet, elle peut être créée et améliorée ... »

Informations précises

« Ce qui nous identifie sur internet (...) Pseudo, adresse mail, identifiant, nom, prénom, date de naissance, âge, adresse »

Composantes

1. Profil sur les réseaux sociaux (88%)
2. Pseudonyme sur les réseaux sociaux (85%)
3. Traces laissées par la personne (80%)
4. Ensemble de tout ce qui se rapporte à la personne sur Internet (76%)
5. Adresse mail (74%)



Partie 2

**A la recherche de moyens d'identification en ligne
socialement acceptables et respectueux des droits et libertés**

Les enjeux liés à l'usurpation d'identité

La CNIL alerte sur une explosion des cyberattaques

Le gendarme des données personnelles a enregistré 5.037 notifications de violation de données en 2021, soit une hausse de 79 % sur un an. Elles concernent notamment près de 2.200 attaques par rançongiciel.

<https://www.lesechos.fr/tech-medias/hightech/la-cnil-alerte-sur-une-explosion-des-cyberattaques-1406384>



ANSSI, Panorama de la cybermenace 2022

Si le nombre d'attaques par rançongiciel est en baisse sur l'année 2022, leurs conséquences demeurent très importantes, plus particulièrement dans des secteurs critiques comme la santé. **Outre les conséquences financières, ce type d'évènement peut également avoir un impact sur le suivi des patients et la confidentialité de leurs données de santé.** Dans la nuit du 20 au 21 août 2022, le Centre Hospitalier Sud Francilien a été victime d'une attaque par rançongiciel revendiquée par le groupe Lockbit. L'indisponibilité d'une partie des données et des applications portées par le système d'information a contraint les services hospitaliers à **fonctionner en mode dégradé**. En outre, le 23 septembre 2022, **11 gigaoctets de données exfiltrées lors de la compromission ont été publiés sur le site web du groupe cybercriminel**. Parmi les éléments divulgués figuraient notamment des données médicales et personnelles liées aux patients et au personnel hospitalier. Une situation similaire s'est répétée quelques mois plus tard au Centre Hospitalier de Versailles.

Victimes - Usurpation d'identité numérique

9,4% (N : 35) des répondants



Les principales formes d'usurpation d'identité

Quelqu'un a utilisé mes données de connexion pour accéder à mes espaces/comptes en ligne	51%
Quelqu'un a utilisé en ligne mes photos/vidéos d'une manière qui ne me plaisait pas	37%
Quelqu'un a créé un faux profil sur moi en ligne	37%
.....	

- **Victimation ponctuelle**
 - Au moins 1 fois au cours des 12 derniers mois : 57%
- **Espace** de victimation :
 - **Réseaux sociaux** (77%)
- **Différences selon le genre** ($p < 0,001$) :
 - Garçons : 5,7%
 - Filles : 13,2%
 - « Autre » : 50%
- Près de 7 victimes sur 10 considèrent l'usurpation d'identité → **expérience négative et blessante**

Auteurs - Usurpation d'identité numérique

6,2% (N : 23) des répondants



Les principales formes d'usurpation d'identité

J'ai utilisé les données de connexion de quelqu'un d'autre pour accéder à ses espaces/comptes en ligne	70%
J'ai créé un faux profil de quelqu'un d'autre en ligne	56%
J'ai utilisé les photos/vidéos de quelqu'un d'autre pour me faire passer pour lui en ligne	52%
.....	

- **Usurpation ponctuelle**

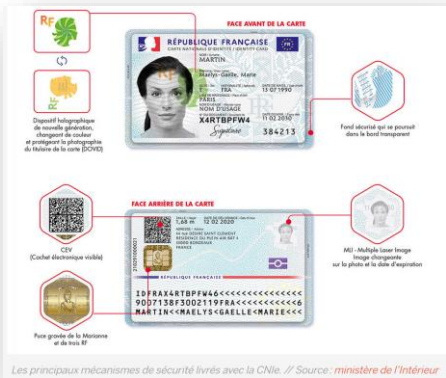
- Au moins 1 fois au cours des 12 derniers mois : 61%

- **Espace** de victimation : **réseaux sociaux** (70%)

- **Différences selon le genre ?** Non

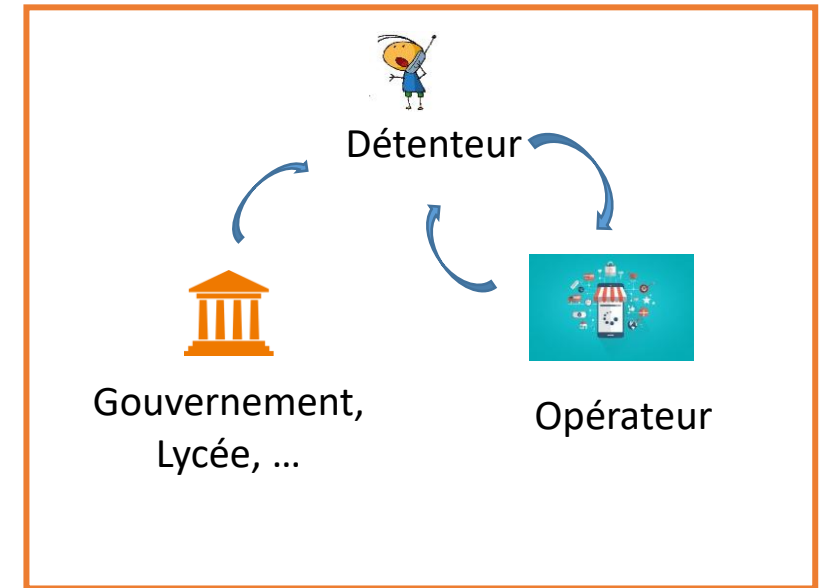
Les moyens d'identification en droit

1 - LA CNIe



Moyens
d'identification

2 - Le portefeuille d'identité numérique (PEIN)



3 - Autres

Service Général
d'Identité
numérique (SGIN)

Sign in with Google

Or

User ID

Password

Login



Points de vigilance :

- Respect vie privée et données personnelles
- Recours à la biométrie

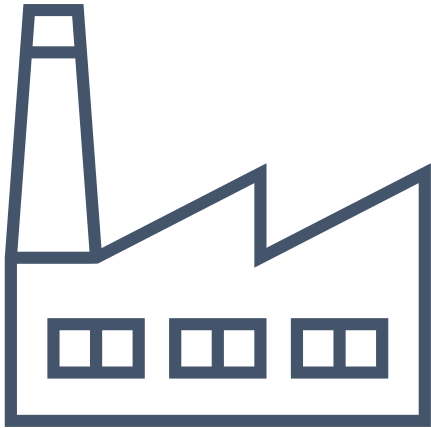
Les moyens d'identification en pratique

Moyen le plus populaire (1 seule réponse)	Identifiant et mot de passe	70%
	Reconnaissance faciale	18%
	Empreintes digitales	9%
Utilisation de ... pour s'identifier en ligne (question à choix multiple)	Données biométriques	89%
	Bouton « s'identifier » de Facebook et Google	76%
	France-Connect	16%
	Blockchain	8%

❖ **Différences selon le genre**

❖ **Différences selon le parcours scolaire**

Entreprise



• 43%

- Fins lucratives
- Peu de transparence concernant modes de collecte et d'utilisation des données
- « *Ce sont mes données personnelles* »

Etat



• 41%

- Surveillance et contrôle
- « *c'est des données personnelles donc mes données elle regarde personne d'autres* »
- Méfiance à l'égard des institutions

Collectivités territoriales



• 27%

- Sécurité données
- « *C'est la même chose que avec l'Etat* »
- « *Ils peuvent nous stigmatisé ou nous mettre dans des cases pour ce que nous sommes* »



Merci

Jessica Eynard

Jessica.eynard@ut-capitole.fr

Giorgia Macilotti

Giorgia.macilotti@irit.fr