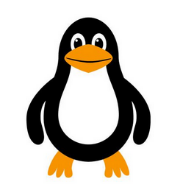
**CEJMA : l’identité numérique de l’organisation**



Le lycée est une organisation : quelle est son identité numérique et comment la préserver ?

Une méconnaissance et/ou une non maîtrise des traces représente pour une organisation un risque économique, juridique, et une atteinte à l’identité de l’entreprise.

A partir des resssources jointes et de vos recherches, **répondez aux 3 MISSIONS**

**Mission 1  : comprendre la notion d’identité numérique**



1. **Faites un état des lieux de l’identité numérique du lycée, en réalisant un « Webmii » sur « le lycée F Le Dantec »,**

Webmii permet d’évaluer le niveau de visibilité sur le web (une note entre 0 et 10 est attribuée)

On trouve : note : Webmii ne peut chercher « lycée F Le Dantec » car il ne prend en paramètres qu’un nom et prénom. (le lycée a une présence moyenne sur le Net)

1. **A partir du site du lycée, recensez des élèments se rapportant à l’identité numérique du lycée F Le Dantec. A quelle composante de l’identité numérique appartiennent les éléments que vous avez trouvés ?**

Déclarative car le lycée les a volontairement saisis.

**Mission 2: identifier les menaces qui pésent sur l’identité numérique**



**Affaire n°1 : une PME victime d’usurpation d’identité (vidéo)**

<https://www.francetvinfo.fr/faits-divers/justice-proces/une-pme-victime-d-une-usurpation-d-identite_1076625.html>

1. **Indiquez les modalités de cette usurpation :**

Les escrocs se sont fabriqués une adresse mail au nom du pdg de l’entreprise, pour obtenir 1,6 millions d’euros de la responsable des finances. Cet argent devait financer l’activité de l’entreprise pour toute l’année et la construction de la médiathèque de la Sorbonne d’Abou Dabi.

1. **Indiquez les conséquences de cette usurpation pour l’entreprise**

Il y a des conséquences :

* + L’entreprise perd tous ses moyens financiers
  + la construction de la médiathèque de la Sorbonne d’Abou Dabi est annulée

**Affaire n°2 : Une fraude très organisée au chômage partiel grâce à une usurpation de l’identité des entreprises**

Le parquet de Paris a ouvert une enquête pour « escroqueries et blanchiment en bande organisée » après des demandes frauduleuses de versement d’indemnités.

Les milliards d’euros débloqués par les pouvoirs publics pour soutenir l’économie ont ouvert l’appétit d’aigrefins. Vendredi 10 juillet, le procureur de la République de Paris, Rémy Heitz, a annoncé, dans un communiqué de presse, que ses services enquêtaient sur des fraudes à l’activité partielle (ou chômage partiel). Ce dispositif, mis en place à très grande échelle depuis la mi-mars pour prévenir les licenciements en cascade, s’est traduit par l’octroi d’aides financières massives, dont une partie – semble-t-il infime, à ce stade – a été détournée.

Les incriminations retenues par le parquet portent sur des chefs *« d’escroqueries en bande organisée »* et *« de blanchiment en bande organisée de ces escroqueries »*. Précision importante : ces infractions ne concernent pas des employeurs qui auraient touché des subsides tout en faisant travailler leurs salariés, théoriquement placés en chômage partiel. Elles renvoient, en l’espèce, à des *« demandes frauduleuses de versement d’indemnités »*, qui ont été déposées en usurpant *« la raison sociale et le numéro d’identification »* d’entreprises existantes – alors même que celles-ci n’avaient jamais effectué une telle démarche.

[**https://www.lemonde.fr/politique/article/2020/07/13/une-fraude-tres-organisee-au-chomage-partiel-grace-a-une-usurpation-de-l-identite-des-entreprises\_6046054\_823448.html**](https://www.lemonde.fr/politique/article/2020/07/13/une-fraude-tres-organisee-au-chomage-partiel-grace-a-une-usurpation-de-l-identite-des-entreprises_6046054_823448.html)

1. **Indiquez les modalités de cette usurpation**

On a trouvé et utilisé le nom (raison sociale) et le numéro d’identification d’entreprises pour toucher les aides au chômage partiel à leur place.

1. **Indiquez les conséquences de cette usurpation pour les entreprises**

Les conséquences sont économiques et juridiques. De plus son image marque est atteinte.

1. **Indiquez sur quoi (sur quel fondement juridique), le procureur de la République de Paris, va-t-il s’appuyer pour faire son enquête.**

Usurpation d’identité basée sur « escroquerie en bande organisée » et « blanchiment en bande organisée de ces escroqueries ».

1. **Indiquez les sanctions qui peuvent être infligées aux fraudeurs.**

Pour escroquerie en bande organisée, les fraudeurs encourent dix ans de prison et un million d’euros d’amende et pour blanchiment d’argent, 750 000€ d’amende et encore dix ans de prison.

**Affaire n°3 : Accès frauduleux dans un système de traitement automatisé de données (STAD)**

**Commentaire du jugement du Tribunal de Grande Instance de Vannes 13 juillet 2005 - Université de Bretagne Sud c/ X**

En résumé, les faits sont les suivants : Quatre étudiants ont été condamnés par le Tribunal de Grande Instance de Vannes pour avoir accédé et s'être maintenu frauduleusement à un système de traitement automatisé de données - STAD (art. 323-1 du code pénal), en particulier en s'introduisant sur les comptes utilisateurs du réseau pédagogique de l'Institut Universitaire de Vannes.

Le Tribunal retient que l'accès et le maintien frauduleux à un STAD sont constitués *« dès lors qu'une personne, non habilitée, pénètre dans ce système tout en sachant être dépourvue d'autorisation, peu importe le mobile ».*

En l'espèce, les quatre étudiants ont téléchargé sur Internet un logiciel de décryptage des mots de passe, ont accédé ensuite sur la base de données regroupant les identifiants et les mots de passe cryptés, puis ont décryptés à l'aide de ce logiciel ces mots de passe pour enfin accéder à certains comptes utilisateurs du réseau pédagogique de l'Institut Universitaire de vannes.

Le Tribunal retient que les quatre étudiants qui ont agi par jeu et défi, ont reconnu connaître le caractère illicite d'une telle introduction dans un STAD du fait de leur signature d'une charte de bons usages des ressources informatiques qui interdit *« de masquer sa véritable identité, d'obtenir le mot de passe d'un autre utilisateur, d'altérer des données ou d'accéder à des informations appartenant à d'autres utilisateurs sans leur autorisation, la réalisation ou l'utilisation d'un programme informatique ayant de tels objectifs ».*

Considérant que ces quatre étudiants, âgés de 18 à 20 ans au moment des faits et jamais condamnés avant, ont fait preuve *« d'une attitude de défi sous une forme technologique propre à la jeunesse sans conséquence préjudiciable pour les comptes utilisateurs usurpés »,* le Tribunal les a condamnés par une peine d'avertissement prenant la forme d'une peine d'amende avec sursis.

En conclusion, la charte informatique est l'un des moyens les plus courants d'informer le personnel d'une entreprise, mais aussi les étudiants et les stagiaires sur les limites d'utilisation d'un STAD.

<https://blogavocat.fr/space/delphine.bastien/content/acces-frauduleux-dans-un-systeme-de-traitement-automatise-de-donnees--stad-_aa84fb96-8cd4-4860-9df6-c9efa2729809>

1. **Précisez ici ce qui a été usurpé dans cette affaire**

Les identifiants et mots de passe des utilisateurs du réseau universitaire de Vannes.

1. **Précisez ce qu’est un STAD . système de traitement automatisé de données**

Selon la définition juridique : *« tout ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciel, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité »* . Un STAD peut donc comprendre toute sorte d’ordinateur, tant client que serveur sur un réseau.

1. **Relevé les modalités d’accès utilisés par les étudiants**

Les étudiants ont accédé à la base de données de mots de passe du serveur, et à l’aide d’un logiciel de décryptage de mots de passe, ont décrypté les mots de passe des comptes utilisateurs. Ensuite ils se sont connectés à ces comptes.

1. **Indiquez sur quoi se base les juges pour qualifier ces fait d’acccès frauduleux à un STAD**

Les juges citent la charte qu’ont signé les étudiants, qui interdit *« de masquer sa véritable identité, d'obtenir le mot de passe d'un autre utilisateur, d'altérer des données ou d'accéder à des informations appartenant à d'autres utilisateurs sans leur autorisation, la réalisation ou l'utilisation d'un programme informatique ayant de tels objectifs »*, et la définition de l’accès et du maintien illégal à un STAD (*« dès lors qu'une personne, non habilitée, pénètre dans ce système tout en sachant être dépourvue d'autorisation, peu importe le mobile »).* Les étudiants n’étaient pas habilités ni autorisés à pénétrer dans le STAD.

1. **Indiquez les sanctions qui ont été infligées, pourquoi sont-elles légères ?**

Les étudiants ne seront sanctionnés que d’une amende avec sursis. Ils n’ont en effet pas nuit aux usagers du réseau universitaire, et pas ouvert de faille de sécurité considérable. Les juges se sont donc montrés commodes, comprenant la simple attitude de défi des étudiants.

1. **Indiquez les sanctions maximales prévues. par le code pénal.**

Deux ans de prison et soixante mille euros d’amende.

**Ressource 1 : qu’est ce que l’identité numérique d’une organisation**



L'identité numérique d’une organisation, est constituée de l'ensemble **des contenus diffusés** sur Internet, des publications et **des traces** laissées sur Internet, **volontairement ou non**, par l’organisation ou par d’autres permettant **d’identifie**r cette organisation.



**Les 3 composantes** de l’identité numérique :

**L'identité déclarative** qui se réfère aux **données saisies** par l'utilisateur comme son nom, son logo, sa dénomination ou raison sociale, son adresse, sa nationalité et sa création. Plus largement, elle englobe toutes les informations que l’organisation décide **volontairement d**e partager sur le web.

Exemple : un article publié sur le site de l’organisation

* **L’IDN** (Internationalized Domain Name, « nom de Domaine internationalisé ») est le **nom de domaine d’une organisation**. Chaque organisation a un IDN unique sur Internet.
* **Les certificats et les signatures électroniques** sont également des éléments d’identification techniques.<https://www.afnic.fr/fr/produits-et-services/services/whois/>

**L'identité agissante** qui est indirectement renseignée par **les activités** de l'utilisateur sur la toile, ce sont les métadonnées, qui permettent de mieux connaître l’organisation à **travers les traces laissées** par celle-ci lors de **ses navigations** ou de ses apparitions sur le web.

**(**Cette facette de l’identité numérique est uniquement le fait des personnes physiques, mais l’ « empreinte digitale » ainsi laissée peut impacter la notoriété de l’entreprise.)

Exemple : les consultations de sites Internet pour la recherche d’un nouveau fournisseur par un membre de l’organisation.

Les éléments permettant de **retrouver les traces** laissées par l’organisation sur le web son l’adresse IP publique, les cookies, les données de géolocalisation ou encore les flux RSS.

**L'identité calculée** qui résulte **d'une analyse de l'identité agissante et déclarative** par le système, elle est forgée par des algorithmes qui interprètent les données collectées pour recomposer les différentes facettes d’une identité. Ces outils extrapolent dans le but de prévoir les besoins et d’y répondre de façon anticipée.

On analyse le nombre de « likes », le nombre de communautés virtuelles dans lesquelles l'individu évolue, ou encore ses fréquentations sur les réseaux sociaux.

Exemple : Le calcul du nombre de connexion sur un site pour présager de l’importance de l’activité de l‘organisation.

Les **cookies** constituent généralement des sources d’informations pour les opérateurs : ils permettent d’anticiper les comportements à venir de l’organisation

**Ressource 2 : l’usurpation d’identité dans une une entreprise**

**Définition :**

L’usurpation d’identité consiste **à utiliser les éléments d’identification** d’une autre personne juridique sans son accord.

L’usurpation peut être :

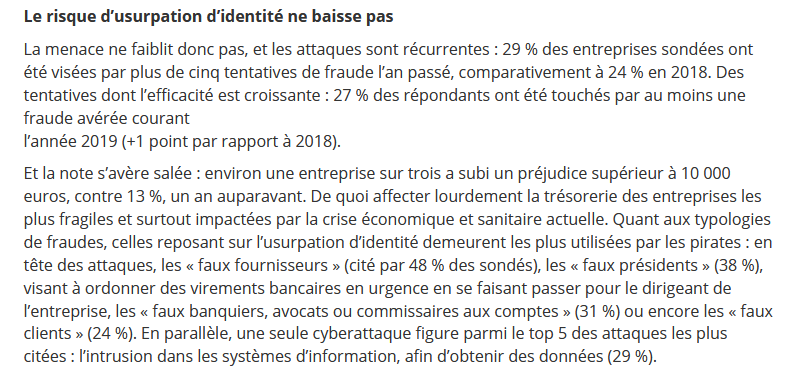
* classique, matérielle (fausse carte d’identité)
* ou en ligne (phishing\*(hameçonnage), faux site web, piratage d’une boite mail…).

Elle est considérée comme un **délit** donc associé à une **sanction pénale**

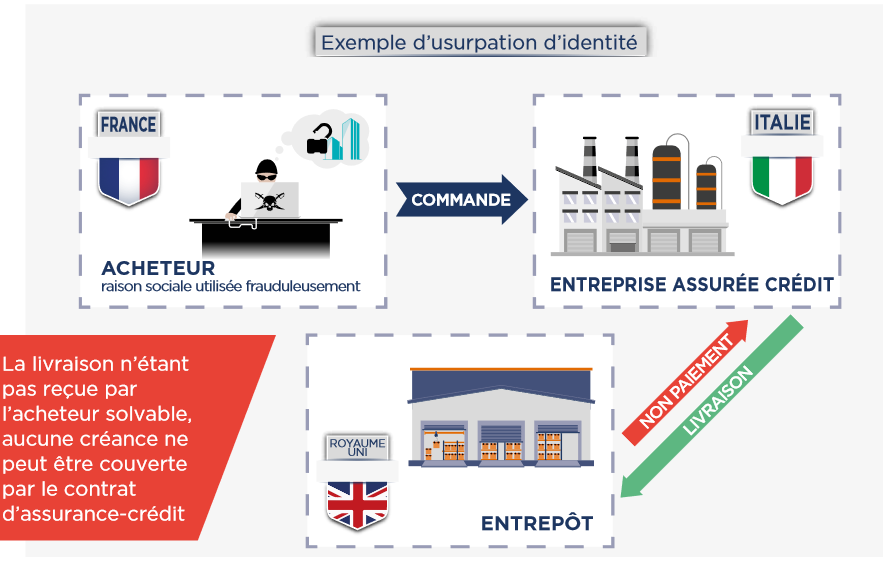
Il peut y avoir **plusieurs types** de délits :

* Délit d’usurpation d’identité numérique,
* Délit d’escroquerie,
* Délit d’accès frauduleux à un système de traitement automatisé de données,

<https://www.cnil.fr/fr/comment-reagir-face-une-usurpation-didentite>



[**https://echos-judiciaires.com/actualite/numerique-cybercriminalite-risque/**](https://echos-judiciaires.com/actualite/numerique-cybercriminalite-risque/) **(26/06/2020)**



**Ressource 3 : les sanctions en cas d’usurpation d’identité : Article 226-4-1 du code pénal**

* Modifié par [LOI n°2020-936 du 30 juillet 2020 - art. 19](https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=80C96BA4F078B09BAE1E620A83FB91AB.tplgfr34s_2?cidTexte=JORFTEXT000042176652&idArticle=LEGIARTI000042181412&dateTexte=20200905&categorieLien=id" \l "LEGIARTI000042181412)

Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.

Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.

Lorsqu'ils sont commis par le conjoint ou le concubin de la victime ou par le partenaire lié à la victime par un pacte civil de solidarité, ces faits sont punis de deux ans d'emprisonnement et de 30 000 euros d'amende.

(Si l’infraction est commise par une personne morale , la sanction prévue passe à 75 000€ d’amende avec une possible dissolution si la personne morale a été créée en vue de commettre l’infraction)

[**https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000023709201&cidTexte=LEGITEXT000006070719**](https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000023709201&cidTexte=LEGITEXT000006070719)

**Ressource 4 : pour prouver le délit d’usurpation d’identité , il faut 2 élèments :**

Comme toute infraction pénale, l’usurpation d’identité numérique nécessite la réunion d’un élément matériel et d’un élément intentionnel :   
**L’élément matériel** c’est l’utilisation de l’identité d’un tiers ou de données de toute nature permettant de l’identifier sur un réseau de communication électronique (nom, prénom ou toute autre donnée permettant l’identification )  
L’élément **intentionne**l c’est la volonté de troubler la tranquillité d’un tiers ou de porter atteinte à son honneur et à sa réputation.



**Ressource 5 : les sanctions en cas d’escroquerie selon le code pénal**

**Article 313-1** [En savoir plus sur cet article...](https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=1F1926932C553F2A35230B221CB05CAC.tplgfr36s_2?idArticle=LEGIARTI000006418192&cidTexte=LEGITEXT000006070719&dateTexte=20200906)

Modifié par [Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002](https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=1F1926932C553F2A35230B221CB05CAC.tplgfr36s_2?cidTexte=JORFTEXT000000219672&idArticle=LEGIARTI000006716442&dateTexte=20000923)

L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manoeuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.

L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende.

**Article 313-2** [En savoir plus sur cet article...](https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=1F1926932C553F2A35230B221CB05CAC.tplgfr36s_2?idArticle=LEGIARTI000028394778&cidTexte=LEGITEXT000006070719&dateTexte=20200906)

Modifié par [LOI n°2013-1203 du 23 décembre 2013 - art. 86](https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=1F1926932C553F2A35230B221CB05CAC.tplgfr36s_2?cidTexte=JORFTEXT000028372809&idArticle=LEGIARTI000028376008&dateTexte=20131225)

Les peines sont portées à sept ans d'emprisonnement et à 750 000 euros d'amende lorsque l'escroquerie est réalisée :

1° Par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission ;

2° Par une personne qui prend indûment la qualité d'une personne dépositaire de l'autorité publique ou chargée d'une mission de service public ;

3° Par une personne qui fait appel au public en vue de l'émission de titres ou en vue de la collecte de fonds à des fins d'entraide humanitaire ou sociale ;

4° Au préjudice d'une personne dont la particulière vulnérabilité, due à son âge, à une maladie, à une infirmité, à une déficience physique ou psychique ou à un état de grossesse, est apparente ou connue de son auteur ;

5° Au préjudice d'une personne publique, d'un organisme de protection sociale ou d'un organisme chargé d'une mission de service public, pour l'obtention d'une allocation, d'une prestation, d'un paiement ou d'un avantage indu.

Les peines sont portées à dix ans d'emprisonnement et à 1 000 000 euros d'amende lorsque l'escroquerie est commise en bande organisée.

**Article 313-3** [En savoir plus sur cet article...](https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=1F1926932C553F2A35230B221CB05CAC.tplgfr36s_2?idArticle=LEGIARTI000006418196&cidTexte=LEGITEXT000006070719&dateTexte=20200906)

La tentative des infractions prévues par la présente section est punie des mêmes peines.

Les dispositions de l'[article 311-12](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006418151&dateTexte=&categorieLien=cid) sont applicables au délit d'escroquerie.

**Ressource 6 : intrusion dans un STAD (système de traitement automatisé de données)**

L'article 323-1 du Code pénal dispose :

* Modifié par [LOI n°2015-912 du 24 juillet 2015 - art. 4](https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=5F125A9D49059F99587CAC1C2827555D.tplgfr36s_2?cidTexte=JORFTEXT000030931899&idArticle=LEGIARTI000030933630&dateTexte=20150727&categorieLien=id" \l "LEGIARTI000030933630)

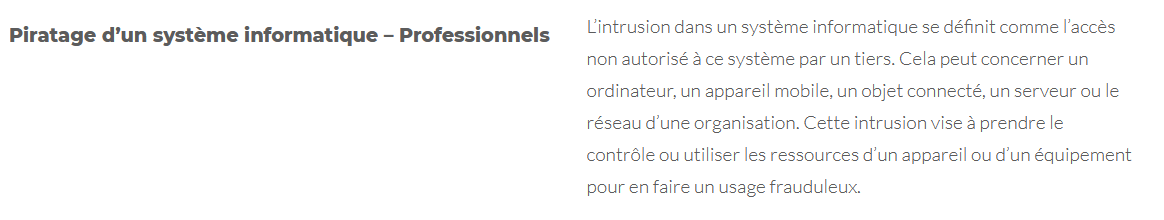
Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni **de deux ans** d'emprisonnement et de **60 000** € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende.

**NB : changement des montants**

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/liste-des-cybermalveillances-traitees-par-lassistant-de-diagnostic>



**Mission 3: réaliser une note d’information à destination du proviseur du lycée**

**TRAVAIL DE GROUPE** : A l’aide de vos réponses et des ressources

Réaliser **une note d’information ou un résumé** destiné au proviseur du lycée F Le Dantec sur le sujet :

Risques et protection juridique de l’identité numérique du lycée

Pour réaliser ce travail, **vous compléterez le wiki qui** est sur **Moodle**

Ce wiki est collaboratif.

Le G1 a un wiki, le G2 a le sien, non visible dans un 1er temps par le groupe adverse.

