MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

ÉduNum
Thématique

eduscol

N°19

Mars 2023

Cette lettre ÉduNum aborde la notion de **cybersécurité** à travers les disciplines et enseignements, en croisant les regards théoriques et en l'illustrant par des pistes d'exploitation pédagogiques. Elle s'adresse à tous les enseignants.

> « J'abrège : vos machines à représenter, à penser, souffriront-elles ? Que peut être le futur pour elles, qui ne sont que mémoires ? »
>
> Jean-François Lyotard, L'Inhumain : Causeries sur le temps, Paris, Galilée, « Débats », 1988

Sommaire

La **stratégie numérique pour l'éducation 2023-2027** repose sur une série de mesures pour renforcer les compétences numériques des élèves et accélérer l'usage des outils numériques pour leur réussite. L'Éducation nationale, précise le texte de présentation, « joue également un rôle déterminant dans la sensibilisation aux enjeux de cybersécurité, qui entre pleinement dans les enseignements numériques tout au long de la scolarité »[1]. Dans la *Revue Défense Nationale*[2], **Marc Watin-Augouard** indique : « Mais à l'heure de l'interconnexion des systèmes, du partage des données, de la domination de géants numériques, aujourd'hui américains et déjà chinois, la souveraineté numérique – celle qui porte notamment sur les réseaux, les informations, les normes – est remise en cause par le caractère extraterritorial et la privatisation du *substrat* numérique ». La cybersécurité, au cœur de cette souveraineté, est ainsi porteuse d'enjeux stratégiques imbriqués de nature multiple : diplomatique (stabilité du cyberespace[3], ingérences étrangères), économique et géopolitique (criticité des métaux stratégiques et des terres rares, contrôle des câbles sous-marins, approvisionnement des semi-conducteurs), juridique (lutte contre la cybercriminalité), environnementale et technologique (écoconception, cyberrésilience), informationnelle (infopollutions) et éducative (formation initiale et continue, découverte des métiers de la cybersécurité).

La cybersécurité fait l'objet en matière de politique française d'une stratégie nationale d'accélération inscrite dans le plan d'investissement France 2030.

REPÈRES

Cybersécurité et sécurité numérique

Nicolas Arpagian indique que la « cybersécurité va donc concerner les usages défensifs et offensifs [des] systèmes d'information qui irriguent désormais nos organisations modernes. Elle prend en compte les contenants, c'est à dire les moyens techniques

[1] Ministère de l'Éducation Nationale et de la Jeunesse. *Numérique pour l'éducation : Vision stratégique 2023-2027*. (2023). https://www.education.gouv.fr/media/120418/download. p.23

[2] Watin-Augouard, M. (2022). La souveraineté numérique à l'épreuve de la métamorphose numérique. *Revue Défense Nationale*, 855, 7. https://doi.org/10.3917/rdna.855.0007

[3] Voir à ce sujet la notion de *splinternet* : Laugée, Françoise. Splinternet. *La rem* n°63 Automne 2022

(réseaux informatiques, téléphoniques, satellitaires...) utilisés pour l'échange de données, qui peuvent faire l'objet d'opérations d'infiltration, d'altération, de suspension, voire d'interruption, comme les contenus, c'est-à-dire l'ensemble des informations qui circulent ou sont stockées sur des supports numériques (informatique industrielle, site Internet, bases de données, messageries et communications électroniques, transactions dématérialisées...) ». La cybersécurité porte ainsi aussi bien selon l'auteur sur « la protection et l'attaque d'équipements informatiques (la guerre pour ou contre l'information), afin de les surveiller ou d'en prendre le contrôle, que sur les renseignements disponibles sur la Toile (la guerre par l'information), avec de possibles atteintes à la réputation, le vol de données sensibles, des actions de piratage numérique et autres campagnes de dénigrement »[4].

L'expression « sécurité numérique » est également employée de manière équivalente pour qualifier la protection des technologies et la prévention des attaques. L'**Organisation de coopération et de développement économiques** (OCDE) apporte toutefois une nuance sémantique : « La sécurité numérique fait référence aux aspects économiques et sociaux de la cybersécurité, par opposition aux aspects purement techniques et à ceux liés à l'application du droit pénal ou à la sécurité nationale et internationale »[5].

Les deux formulations seront utilisées dans la présente lettre. Le **Commissariat à l'Énergie Atomique et aux Énergies Alternatives**, offre ci-dessous un aperçu graphique des niveaux d'intervention et des actions de cybersécurité en matière d'analyse des vulnérabilités et de protection des systèmes. L'infographie « Plongée dans les profondeurs de la cybersécurité » est extraite du site web du **CEA** qui consacre un dossier complet à la cybersécurité.

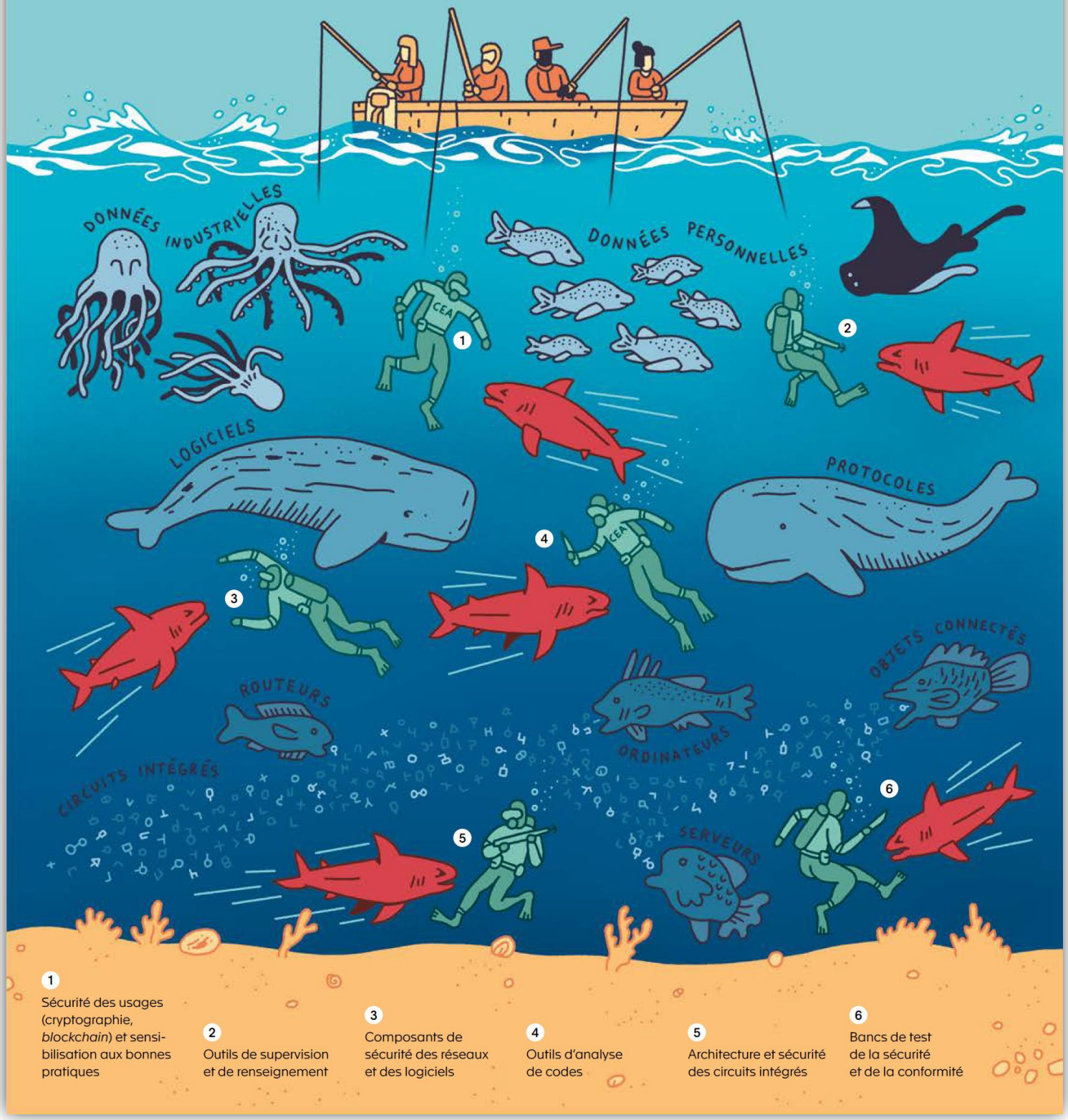
[4] Arpagian, Nicolas. *La cybersécurité*. 3e éd. Mise à jour, Que sais-je ?, 2018. p.9-10

[5] « Sécurité numérique ». *OCDE* [en ligne]. [Consulté le 7 janvier 2023]. Disponible à l'adresse: https://www.oecd.org/fr/numerique/ieconomie/securite-numerique

Plongée dans les profondeurs de la cybersécurité…

« Le cyberespace est d'une complexité telle que sa protection concerne un ensemble de couches numériques interconnectées aussi profond que la Fosse des Mariannes ! Les utilisateurs rament alors sur ce vaste océan qui grouille de requins en tous genres ».

C'est ainsi que Florent Kirchner, chef de département au CEA-List, image la cybersécurité. Et c'est à tous ces niveaux que les équipes du CEA interviennent avec des technologies et des outils qui contribuent à sécuriser notre société désormais numérique.



1 Sécurité des usages (cryptographie, *blockchain*) et sensibilisation aux bonnes pratiques

2 Outils de supervision et de renseignement

3 Composants de sécurité des réseaux et des logiciels

4 Outils d'analyse de codes

5 Architecture et sécurité des circuits intégrés

6 Bancs de test de la sécurité et de la conformité

Les Défis du CEA No 242. Mars-Avril 2021. p.23 - ***© CEA/J. Perrodeau***

Éducation et cybersécurité

Le portail national **éduscol** rappelle que la sécurité numérique est un terme parapluie couvrant un grand nombre de thématiques dont la gestion des mots de passe, la sécurité des appareils mobiles, l'identification de virus, la cryptographie, le chiffrement, la sécurité des données notamment les données personnelles, les courriels indésirables, le piratage de compte, l'hameçonnage, le rançongiciel, l'usurpation d'identité, la protection de son identité en ligne, la gestion des témoins de connexion, la protection de la vie privée… On trouvera dans le document (image-lien ci-dessus) des **références** à cette question dans les **programmes de disciplines et d'enseignements**.

Ajoutons à ces repères le référentiel de compétences sur la sécurité de l'environnement et des pratiques numériques réalisé par **Pix** en partenariat avec l'**ANSSI** et **Cybermalveillance**, à destination des professionnels de l'enseignement et de la formation pour les appuyer dans l'accompagnement de leurs apprenants.

Éduquer au droit à la protection des données

Le référentiel CNIL de formation des élèves à la protection des données personnelles comporte 9 domaines déclinés eux-mêmes en sous-compétences. L'élaboration d'un socle commun de compétences concrètes et pratiques en matière de droits et responsabilités numériques constitue un enjeu éducatif majeur, notamment avec l'application du règlement européen sur la protection des données personnelles (RGPD) dont la **Commission nationale de l'informatique et des libertés** rappelle qu'il est « le seul texte à imposer des obligations de cybersécurité précises, de

façon transversale, et soumises au pouvoir de contrôle et de sanction d'une autorité administrative telle que la CNIL ».

PRATIQUES ET RÉFLEXIONS PÉDAGOGIQUES

Économie de l'attention et de la traçabilité

Un certain nombre de scénarios abordent la question de la sécurité numérique, en particulier en lien avec le domaine 4 « Protection et sécurité » du **Cadre de référence de compétences numériques** (CRCN). Les cahiers IP 6 de la CNIL soulignent le développement d'une hypervigilance attentionnelle qui incite les usagers du web à répondre aux sollicitations visuelles et sonores (cf. scénario bisontin sur les sollicitations numériques), aux incitations douces[6] (séquence de l'académie de Lille) et trompeuses (déjouer les *dark patterns*, académie de Besançon).

Dans le cadre d'un partenariat avec **Terra Numerica**, l'académie de Nice distille une démarche globale en associant élèves, enseignants et scientifiques à une réflexion sur les mécanismes sous-jacents à l'univers des données personnelles et des algorithmes, ainsi qu'à leur explicitation. Rendre visible l'invisible pour ainsi dire…

Sousveillance

Dans le contexte actuel de « datafication » numérique de l'ensemble de nos activités, la question de la **protection** est essentielle face à la **surveillance** permise par la collecte des **données personnelles**. Le terme de « surveillance » n'est pas le seul à être employé dans ce cadre : les formes de « veillance » sont en effet multiples, subies, volontaires ou militantes (autoveillance, coveillance, dataveillance, équiveillance, sousveillance, uberveillance, etc.) et peuvent potentiellement être à l'origine de « mal-veillance » ou

[6] Voir la notion de *nudge* : Laugée, Françoise. Nudge. *La rem* n°49 Hiver 2018-2019

de « bien-veillance ». On saisit alors pleinement la nécessité de protéger le patrimoine informationnel des personnes des atteintes à leurs données, voire à leurs intimités numériques. Le web social, souligne **Jean-Paul Fourmentraux**, est ainsi devenu le « creuset d'une traçabilité sans précédent des comportements, de l'expression des goûts et des dégoûts, et par extension, de l'ensemble des communications et relations interhumaines médiées »[7]. **Bernard Harcourt**[8], poursuit l'auteur, y voit une « mortification de soi », un renoncement à la liberté individuelle, une « servitude volontaire ». En réaction, certains artistes promeuvent la sousveillance comme **Trevor Paglen** dans *Sight machine*, **Paolo Cirio** dans *Street ghosts* (en recourant au mode opératoire des « médias tactiques ») ou **Christophe Bruno** avec le *Dadamètre*.

La sousveillance est une stratégie consistant à surveiller celui qui surveille. Ce dispositif en miroir donne la possibilité à ceux qui le pratiquent de reprendre le pouvoir d'agir sur les technologies intrusives. La sousveillance est donc un regard « du dessous », souhaitant contrer la toute-puissance d'un regard scrutateur provenant « du dessus ». Cette stratégie horizontale donne la possibilité de regarder d'en bas les technologies algorithmiques prédictives et leurs usages potentiellement dangereux pour les libertés individuelles.

Banksy, CC BY-SA 2.0, via Wikimedia Commons

L'artiste **Banksy**, le fer de lance de cette sousveillance, a réalisé de nombreuses œuvres d'art dans l'espace urbain dénonçant la vidéosurveillance. *One nation under CCTV* réalisé sur un mur londonien crée une mise en abyme entre un petit garçon peignant au rouleau les larges lettres « ONE NATION UNDER CCTV » sur le mur filmé par un policier

[7] Fourmentraux, J.-P. (2020). *AntiDATA : La désobéissance numérique: art et hacktivisme technocritique*. Les Presses du réel. p.60-61

[8] « La société d'exposition » : https://www.radiofrance.fr/franceculture/podcasts/la-grande-table-idees/bernard-harcourt-cette-societe-d-exposition-est-une-societe-de-servitude-volontaire-par-la-seduction-7785696

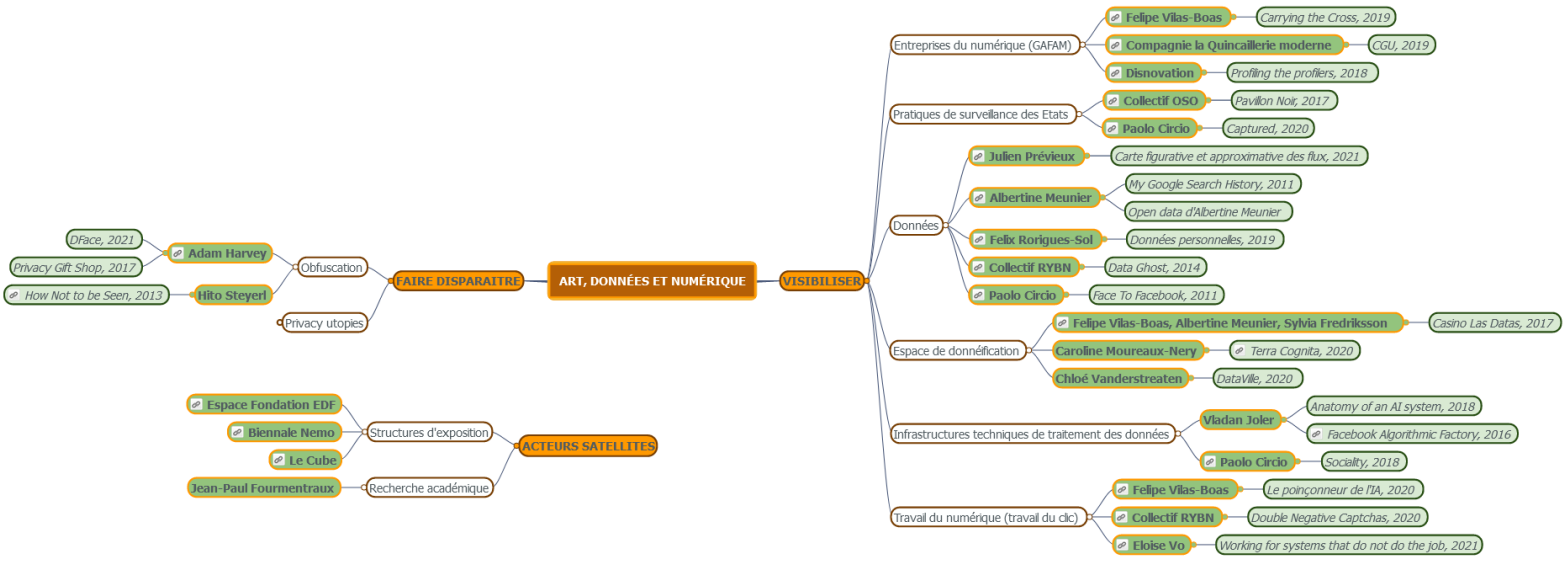
fictif en trompe-l'œil. Toute cette scène étant captée par la vidéosurveillance urbaine londonienne filmant la scène, elle constitue une dénonciation des dérives de ladite vidéosurveillance généralisée à Londres.

Il réitère ce type d'intervention textuelle, dans l'espace public, avec son œuvre londonienne *WHAT ARE YOU LOOKING AT?* (Qu'êtes-vous en train de regarder?) sur laquelle pointe l'objectif d'une caméra de surveillance. Cette œuvre contestataire et engagée est aussi une forme de mise en garde contre les dérives possibles de la vidéosurveillance.

L'exposition *CTRL [Space]* au **ZKM** (Centre d'art et de technologie des médias de Karlsruhe) en 2002, un an après les attentats du 11 septembre 2001, proposait un tour d'horizon des artistes engagés dans des pratiques artistiques incluant la vidéosurveillance et développant une réflexion sur l'émergence de nombreux dispositifs de contrôle. Ces artistes usant de ce médium, face à l'avènement d'une nouvelle ère de contrôle généralisé, font émerger des contre-rôles sans précédent.

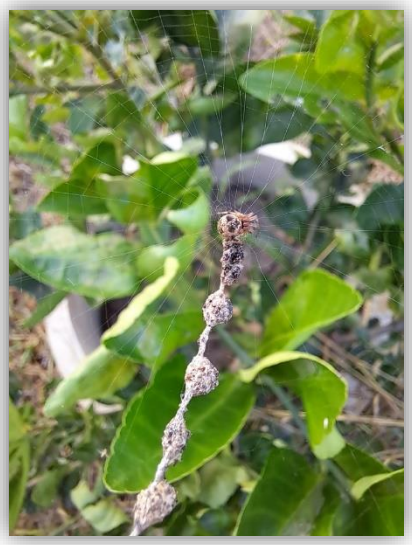
Obfuscation

Ci-dessous une cartographie collaborative et évolutive de l'art des données personnelles élaborée par le **Laboratoire d'innovation numérique de la CNIL (LINC)** permet de



visualiser les différents acteurs et les pratiques de cet « art orienté vers la *visibilisation* et la critique des infrastructures numériques ».

Déjouer le traçage peut aussi s'opérer par d'autres stratégies, notamment l'obfuscation consistant « à produire délibérément des informations ambiguës, désordonnées et fallacieuses et à les ajouter aux données existantes afin de perturber la surveillance et la collecte des données personnelles »[9].



naritsara, Cyclosa mulmeinensis, iNaturalist (CC BY-NC)

L'obfuscation est donc une stratégie de camouflage opérant par saturation, aveuglant les systèmes algorithmiques. Elle fait référence à des systèmes de défense militaire eux-mêmes inspirés des stratégies de défense arachnéennes. Elle est une forme de résistance face aux flux continus informationnels qui placent l'individu en position d'infériorité. Cette technique met en évidence des enjeux éthiques et moraux permettant de redonner à l'individu le pouvoir d'agir afin de préserver sa vie privée en ligne.

Vincent Dubois, dans son œuvre *Undefined.io*, développe un site web permettant aux internautes de poster du contenu sur les comptes des utilisateurs présents sur différents réseaux sociaux. Il donne également la possibilité de télécharger une extension pour navigateur afin d'agir sur notre activité en ligne en générant des requêtes fantômes. Il cherche ainsi à nous faire échapper au profilage qui s'opère en ligne et de mieux comprendre le fonctionnement du numérique systémique.

Leonardo Selvaggio dans son œuvre intitulée *Urme surveillance* participe à cette pratique du brouillage et de camouflage des traces numériques par la création d'un masque modélisant son visage, proposé à ceux souhaitant échapper aux caméras de surveillance à reconnaissance faciale.

[9] Nissenbaum, H., Brunton, F., Marconi, E., & Chemla, L. (2019). *Obfuscation : La vie privée, mode d'emploi*. C&F éditions. p.20

Hacking éthique : fais-le toi-même

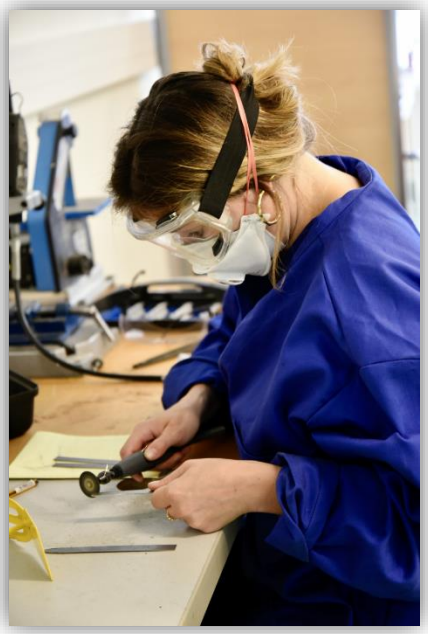
La figure du *hacker* ne renvoie pas systématiquement aux délinquants du numérique, mais aussi à celle du bricoleur créatif. Dans cette perspective, il s'approprie les outils numériques souvent dans une approche critique et, parfois, une démarche de détournement. De surcroît, un *hacker* éthique « orienté art » se situe potentiellement dans la lignée du mouvement *Arts and Crafts* et leur approche artisanale collaborative de l'art.

Michael Förtsch, CC BY-SA 4.0, via Wikimedia Commons. Steve Wozniak im November 2018 - MQ Summit, Ingolstadt

La figure du *hacker* a émergé avec l'avènement du numérique et des réseaux sociaux. Le *hacking* éthique, idéologie sur laquelle repose l'identité du cyberactiviste, s'ancre dans une dimension critique et créative remettant en question un ordre établi hiérarchisé et figé, potentiellement présent dans le cyberespace. Cette dimension est au fondement même de l'avènement du logiciel libre donnant accès aux codes sources, souhaitant ainsi rendre le pouvoir d'agir au plus grand nombre sur les technologies numériques.

Pratiques artistiques technocritiques

Réseau Canopé se saisit de cette éthique du fouineur et de cette démarche créative collaborative en proposant des *hackathons* à destination des équipes éducatives. Ces dispositifs d'une durée variable en présence ou à distance engagent un groupe à résoudre une problématique collectivement pour produire des idées innovantes et originales.



Nicolas Taffin CC BY-NC-SA

L'**ENSCI**, l'école nationale supérieure de création industrielle, a créé la seconde édition de son Créartathon qui reprend cette dynamique collaborative horizontale afin de faire émerger des formes nouvelles dans la création industrielle.

Le « *hacking* éthique » est adopté par certains artistes du **Net art** souhaitant questionner les systèmes algorithmiques marchands permettant de profiler les internautes. L'artiste **Christophe Bruno** a manipulé la technologie de *Google* dans son œuvre en ligne intitulée *Google AdWords Happening23* afin de parasiter et détourner leur système publicitaire. Cette performance en ligne donne à réfléchir sur les pratiques cachées de la firme américaine Alphabet qui, plus qu'un moteur de recherche, peut être considérée comme la plus grande régie publicitaire au monde.

Wikipedia

Antoine Chapon et **Nicolas Gourault**, dans leur installation *Faces in the Mist*, détournent l'usage d'un programme de reconnaissance faciale dans le but de lui faire détecter des masses nuageuses captées sous la forme de flux informels qu'ils associent à des personnalités climato-sceptiques. Cette rencontre formelle impromptue et poétique questionne la fiabilité de ces technologies de surveillance de masse.

C'est dans cette dynamique critique des systèmes informationnels soutenue par les structures numériques que s'inscrit l'artiste Julien Prévieux. Il interroge les techniques de surveillance et de captation de notre attention. Le protocole qu'il utilise dans son œuvre tissée, réalisée pour la CNIL, s'appuie sur la technologie de l'oculométrie visant à capter les mouvements de l'œil, issue de la mercatique permettant d'optimiser l'impact de la publicité en ligne. Cette technologie de surveillance est détournée par l'artiste : son intention est de représenter le flux permanent des atteintes à la protection des données en ligne à laquelle la CNIL doit faire face.

Hacking cindynique

Gaël Musquet est un *hacker* et météorologue français. Il est particulièrement impliqué dans l'anticipation, la prévision et la prévention des catastrophes naturelles en s'inscrivant aussi dans une démarche éthique de piratage. Dans le cadre du **Séminaire de formation cybersécurité NSI Campus Cyber** il présente diverses activités réseau en « scannant » les machines de son univers domestique à partir d'un simple nano-

ordinateur de type **Raspberry Pi**. L'intégralité de son intervention peut être consultée sur la chaîne **PodEduc MENJ - Campus Cyber** et complétée par l'écoute d'un épisode audio de l'émission *Le code a changé* sur France Inter présenté par **Xavier de La Porte**.

Former à la protection des données en arts plastiques

Protéger ses données personnelles ainsi que sa vie privée est actuellement un enjeu majeur au sein de l'enseignement. Cette prise de conscience contemporaine engage toute la communauté éducative. Dans l'**enseignement des arts plastiques**, ce regard critique, porté sur les usages du numérique et les risques qui en découlent, est travaillé dans le projet de l'élève invité à hybrider pratique plastique et numérique. Elle apparaît dans les programmes d'arts plastiques au cycle 4 comme une compétence disciplinaire à maîtriser : *Prendre en compte les conditions de la réception de sa production dès la démarche de création, en prêtant attention aux modalités de sa présentation, y compris numérique.*

Projets pédagogiques

Les **TraAM** (travaux académiques mutualisés) d'arts plastiques de l'académie de Caen ont questionné l'usage du numérique en classe et en dehors de la classe, engageant les élèves dans une réflexion sur leurs usages au quotidien des réseaux sociaux et sur la protection de leur vie privée en ligne.

Nous sommes suivis ! constitue une exemple similaire : il s'agit d'un parcours de sensibilisation multimédia, interactif et modulable à destination des élèves de cycle 4 mis en ligne par la DANE de l'**académie de Nancy-Metz**. Il permet de développer le regard critique des élèves sur l'importance de protéger ses données personnelles en ligne.

Le projet *Arts plastiques et Big Data : 24 heures dans ma vie* s'inscrit dans la même perspective : il engage des élèves de cycle 4 en réseau d'éducation prioritaire sur un questionnement autour de la représentation de soi dans un monde où le numérique transforme et démultiplie leurs identités. Cette réflexion sur l'identité numérique

polyphonique soulève des interrogations sur la trace, l'empreinte, qui est laissée en ligne dans leurs usages d'internet. Une analogie est effectuée entre les gestes produits par les élèves durant 24 heures de leur vie et les données qu'ils partagent durant ces mêmes 24 heures. Ce projet rend visible ces traces par la performance et sa captation vidéographique.

D'autres ressources de (d'auto)formation peuvent être convoquées comme la conférence de sensibilisation *Je n'ai rien à cacher* de **Julien Vaubourg** (Université de Lorraine, 2015) à destination de la communauté éducative ou le *MOOC CHATONS*, cours en ligne ayant pour visée de tracer les contours d'un internet responsable, citoyen et d'un web décentralisé, loin de l'hégémonie des grandes plateformes marchandes numériques.

Au-delà de la sphère du numérique éducatif

Des acteurs du web, s'érigeant contre une hégémonie des plateformes marchandes dans le cyberespace, se saisissent de ces enjeux afin de promouvoir un internet plus libre. Un outil numérique intitulé *respectemesdata.fr* à destination des internautes a été créé dans le cadre de la journée européenne de la protection des données par *UFC Que Choisir*. Il permet d'identifier les données partagées par les usagers avec les plus grandes plateformes du web.

Les artistes, les théoriciens de l'art, des musées et des centres d'art se sont emparés de ces problématiques. Leurs approches articulent les dimensions artistiques aux débats sociétaux et démocratiques. Elles rejoignent, en partie, des préoccupations éducatives plus globales relatives au numérique, aux réseaux sociaux, au cyberespace, à l'éducation aux médias et à l'information, à la lutte contre le harcèlement, etc.

À titre d'exemple, l'exposition *Open Codes. We are Data* organisée par le **ZKM** analyse notre environnement numérique interconnecté composé d'intelligences programmées. L'exposition nous interpelle sur la place prépondérante des algorithmes dans la collecte et le traitement des données. Elle

trace des perspectives saisissantes en modélisant des univers hybridant réalité et fiction, tout en éveillant nos consciences face à la surveillance généralisée rendue possible par ces technologies prédictives.

Protection, sécurité, surveillance technologiques en histoire des arts

Les artistes interrogent le monde dans lequel nous vivons et nos vies intérieures. De nos angoisses, l'art est souvent le dépositaire et plusieurs institutions culturelles ont fait de la cybersécurité un objet culturel.

Les enjeux politiques des technologies de surveillance et d'identification sont soulevés sur le mode des dystopies dans *Les portes du possible. Art et science-fiction* au **Centre Pompidou Metz**, une exposition qui mêle art, littérature et science-fiction. Le deuxième chapitre expose un futur dystopique, « l'algorithmisation » croissante de nos vies sous la forme d'une aliénation et d'une instrumentalisation de nos possibles, les réseaux sociaux décryptant nos modes de vie pour mieux diriger nos désirs et choix à venir. Le travail de l'artiste américain Tishan Hsu, exposé à la Biennale de Venise en 2022 est mis en exergue, révélant les technologies qui désincarnent et connectent simultanément les êtres humains, transforment les corps et les identités avec une attention particulière au mode opératoire. À l'origine de ses travaux se trouve la question des effets de la technologie qu'elle soit déformante, de surveillance ou vivifiante.

BALISES
Le magazine de la Bpi

Cette exposition s'inscrit dans l'histoire du Centre Pompidou, en lien avec les technologies nouvelles apparues depuis les années 70 et contemporaines de son inauguration en 1977. En 2009, une table ronde *Enjeux des politiques d'identification et de surveillance* questionne déjà la traçabilité des informations, l'utilisation des fichiers informatiques, la diffusion de données personnelles, la confidentialité, la préservation de l'intimité et le respect de la démocratie. La tentation totalitariste sous le prisme du réseau est dénoncée par les artistes dans l'exposition *Réseaux monde*. Avec ses sociogrammes en réseaux, l'artiste américain Mark Lombardi explore les structures labyrinthiques du pouvoir politico-économique à l'heure de la mondialisation.

Qu'advient-il lorsque la confidentialité et la préservation de l'intimité sont niées ? C'est ce qu'interroge l'artiste américaine Julia Scher sous une forme parodique en réinvestissant la figure du chien de garde. Julia Scher fait de la surveillance une forme d'art en questionnant le sacrifice des libertés individuelles au nom d'une exigence de protection. Pour finir, les artistes contemporains sont-ils devenus les *hackers* d'aujourd'hui ? L'artiste Cornelia Sollfrank dès 1997 s'insurge contre la prédominance masculine du premier concours en ligne de Net.art (organisé par la Kunsthalle de Hambourg) et pirate ce dernier en générant trois cents faux profils d'artistes femmes au nom de l'égalité.

Topographie et topologie en histoire-géographie

L'**histoire-géographie** apporte son propre éclairage en s'intéressant à l'internet comme territoire (essai de cartographie ci-dessous). Pour paraphraser **Jane Stowell** les données ne sont pas dans les nuages mais dans l'océan, ce qu'illustre le scénario poitevin dédié à la matérialité sensible du numérique et en particulier aux infrastructures câblières[10].

Les conflictualités à l'œuvre dans le cyberespace font l'objet d'un traitement pédagogique au sein de la spécialité **histoire-géographie, géopolitique et sciences**

[10] Consulter l'émission des *Dessous des cartes* : « Câbles sous-marins : la guerre invisible » et cet article de *La rem* (2022)

politiques (HGGSP) : l'académie de Toulouse publie à cet égard une approche axée sur ces aspects (guerre numérique, guerre d'information, guerre hybride) à travers l'analyse d'une série télévisuelle. Dans cette séquence les élèves identifient les réseaux, acteurs et territoires du cyberespace puis réfléchissent aux enjeux de la cyberdéfense[11], notamment en France. La topographie rejoint à ce niveau la topologie et celle(s) des réseaux qui sont étudiées dans les contenus d'enseignements de Sciences numériques et technologie (SNT) en classe de seconde et de la spécialité Numérique et sciences informatiques (NSI)[12].

De la topologie à la cryptologie

Thomas de Leu. Blaise de Vigenère - Wikipedia (DP)

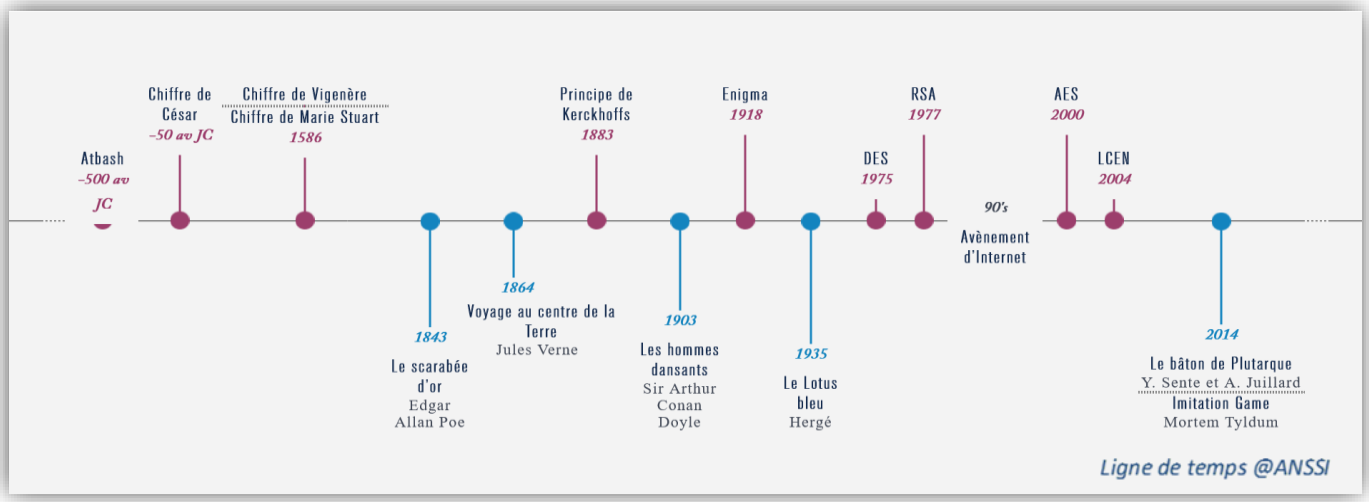
Ce programme de NSI en terminale intègre une entrée « Architectures matérielles, systèmes d'exploitation et réseaux » dans laquelle est abordée la « sécurisation des communications », ce qui implique de s'intéresser au chiffrement et plus largement à la cryptologie.

Étymologiquement, précise la CNIL, la cryptologie est la science (λόγος) du secret (κρυπτός). Elle réunit la cryptographie (« écriture secrète ») et la cryptanalyse (étude des attaques contre les mécanismes de cryptographie). La cryptologie regroupe quatre principales fonctions : le hachage (empreinte unique calculable et vérifiable souvent matérialisée par une longue suite de chiffres et de lettres précédées du nom de l'algorithme utilisé, par exemple « SHA2 » ou « SHA256 ») avec ou sans clé, la signature numérique (vérification de l'identité de l'auteur d'un document) et le chiffrement symétrique, asymétrique ou hybride. Un documentaire de l'**Agence nationale de la**

[11] « La **cyberdéfense**, quant à elle, regroupe également démesures mises en œuvre pour maintenir un état de cybersécurité, mais face à une adversité particulièrement marquée et dans une temporalité bien spécifique : un évènement non désiré survient ou est susceptible de survenir à brève échéance ». Salamon, Y., Poupar, G. (préface). (2020). *Cybersécurité et cyberdéfense : Enjeux stratégiques*. Éditions Ellipses. p.113

[12] Voir concours des **Trophées NSI** : https://eduscol.education.fr/3532/les-trophees-nsi-numerique-et-sciences-informatiques

sécurité des systèmes d'information (ANSSI) permet de découvrir les grandes phases de cette longue histoire[13].



En **mathématiques** le concours Alkindi, ouvert et accessible aux classes de 4e, 3e et 2de, répond aux enjeux de sécurité de l'information en faisant découvrir de façon ludique les fondements mathématiques, informatiques et logiques de la cryptanalyse.

L'analyse fréquentielle (dont la technique est présentée dans le *Manuscrit sur le déchiffrement des messages codés* du polymathe arabe **Al-Kindi**) est traitée dans un scénario de l'académie d'Amiens issu des TraAM 2016-2017. D'autres méthodes comme le chiffrement RSA sont également abordées (académie de Grenoble). Plus globalement, les TraAM 2015-2016 en mathématiques de l'académie de Rennes s'intéressent à la construction de codes secrets en classes de 4e et de 3e.

Contemporaine dans son apparition de la cryptographie, la **stéganographie** (utilisée dans les cyberattaques) désigne l'ensemble des techniques permettant de transmettre une information en la dissimulant au sein d'un autre support, l'objet conteneur et son message caché formant un stégo-objet. L'**académie de Rennes** publie, à titre d'illustration pédagogique, une séquence *ad hoc* dans le cadre de l'enseignement SNT.

[13] Voir également : https://culturemath.ens.fr/thematiques/lycee/voyage-au-coeur-de-la-cryptographie

Le renseignement d'origine sources ouvertes (ROSO)

Le renseignement de source ouverte « est celui qui est accessible, gratuitement ou non, parce que la personne ou l'institution qui le détient le met à disposition du public »[14]. Il s'intègre dans le vaste écosystème du renseignement (essai de carte conceptuelle ci-dessous, p.19) et s'inscrit dans le cadre de l'éducation à la défense[15].

Les techniques « OSINT » peuvent aider les individus à affiner leur stratégie de recherche d'information, à connaître les bases de données disponibles, parfois sous certaines conditions, à évaluer le degré de fiabilité d'une information et pour les organisations à identifier les vulnérabilités dans le but de se prémunir contre d'éventuelles cyberattaques.

Selon **Olivier Le Deuff**[16], le ROSO « constitue un socle commun de compétences et de savoirs entre diverses professions (l'agent de renseignements, le journaliste, le documentaliste, l'archiviste, le chercheur, le *hacker*, etc.)[17] qui manient documents et informations au quotidien. Le but est de pouvoir valoriser l'information et donc de réaliser des processus d'extraction de connaissances. [...] Il repose sur une galaxie hyperdocumentaire dans ses logiques d'extraction, de collecte et de catégorisation, mais aussi d'interrelations et de productions de nouveaux documents ».

Un domaine là encore à explorer dans le cadre de l'enseignement **EMI**, **éducation aux médias et à l'information** en tenant compte des contraintes éthiques et juridiques inhérentes au renseignement. Dans le cyberespace des conflictualités « l'analyse des sources ouvertes est un des instruments de connaissance et de lutte contre les manipulations de l'information » souligne **Alexandre Alaphilippe**[18].

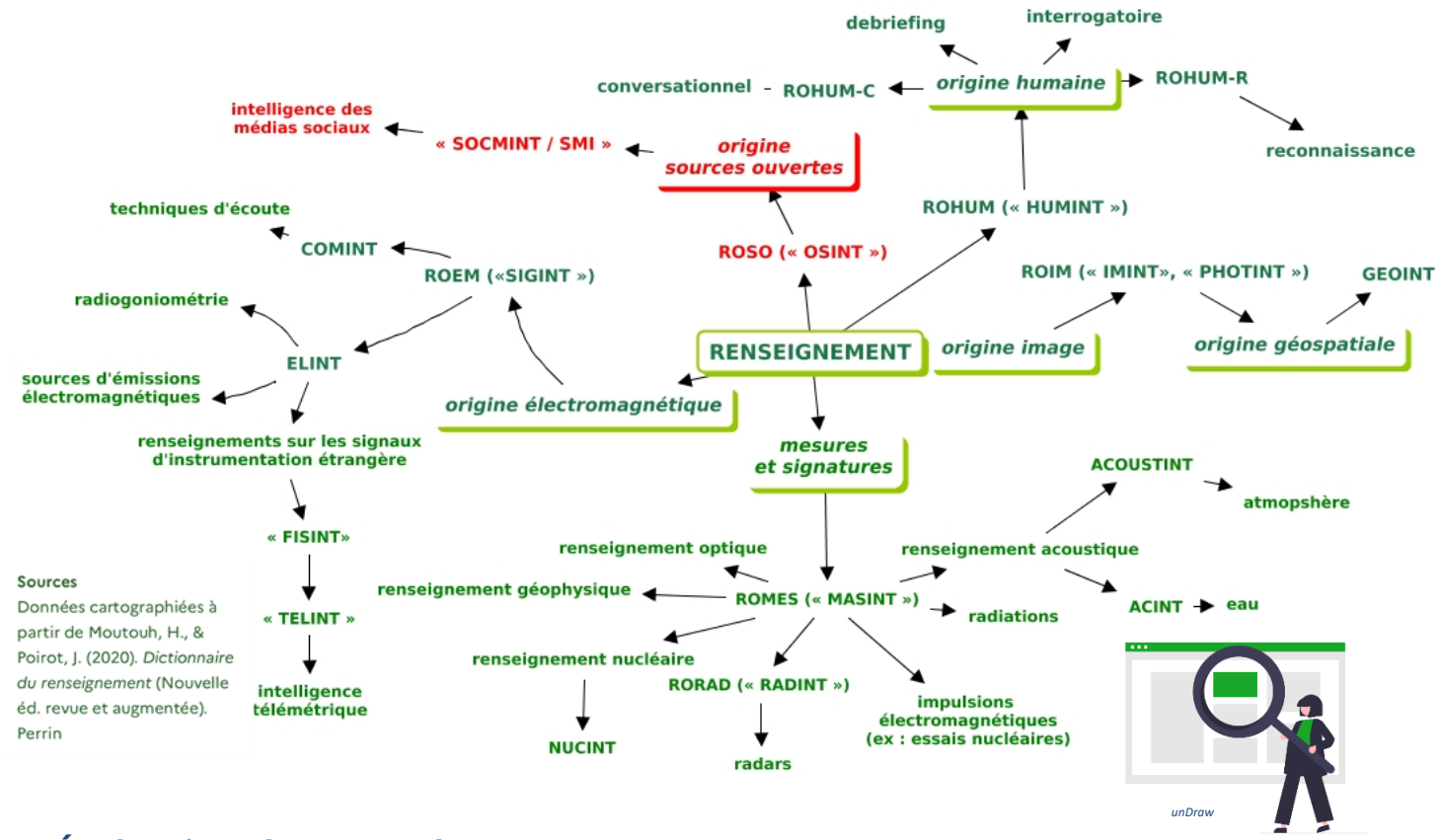
[14] Moutouh, H., & Poirot, J. (2020). *Dictionnaire du renseignement* (Nouvelle éd. revue et augmentée). Perrin. p.1109https://edubase.eduscol.education.fr/fiche/21220

[15] Consulter les Entrées « défense » dans les programmes scolaires et les thématiques, notamment le document Enseigner l'histoire de la guerre, Enseigner la guerre dans l'histoire, Enseigner la guerre au présent

[16] Le Deuff, O. & Roumanos, R. (2021). Open Source Intelligence (OSINT) : retour aux sources. *I2D - Information, données & documents*, 1, 8-12. https://doi.org/10.3917/i2d.211.0008

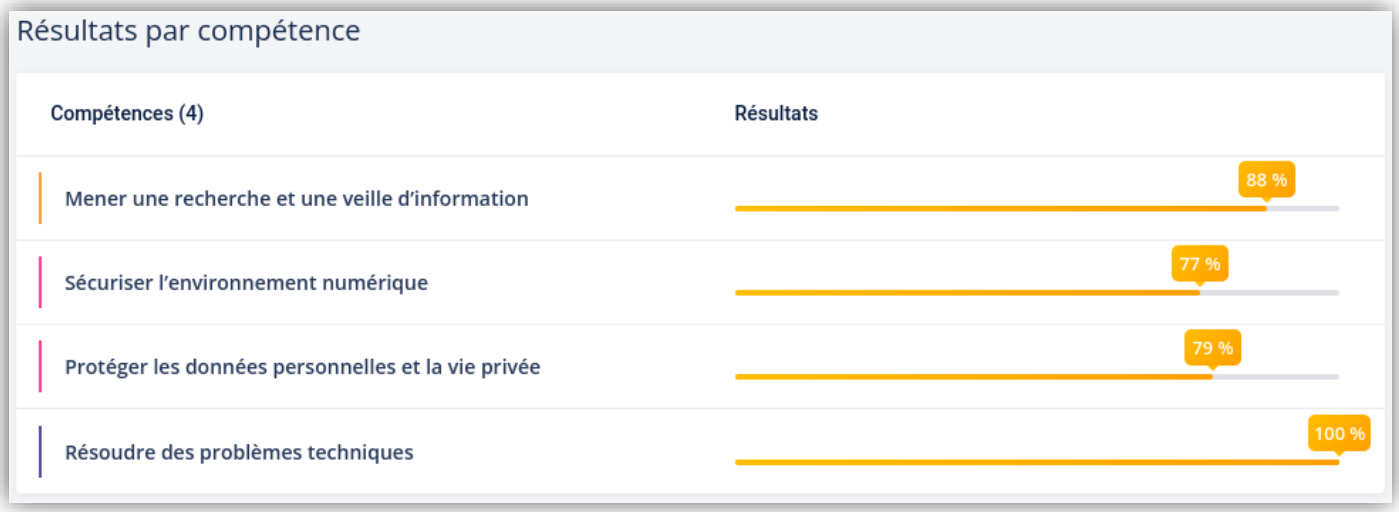
[17] L'Osintosphère permet de visualiser les différents acteurs et leurs éventuels liens

[18] Alaphilippe, A. (2022). « Sources ouvertes et lutte contre la désinformation : un chantier démocratique ». *Hérodote*, 186, 69-83. https://doi.org/10.3917/her.186.0069



Évaluation des compétences

La plateforme **Pix** d'évaluation, de développement et de certification des compétences numériques propose une campagne pour le cycle 4 sur le thème de la cybersécurité. Cette campagne va permettre aux élèves de valider à différents niveaux, 4 compétences du CRCN à savoir, mener une recherche et une veille d'information, sécuriser l'environnement numérique, protéger les données personnelles et la vie privée, résoudre des problèmes techniques. À partir de la plateforme **PixOrga**, l'enseignant peut visualiser les résultats obtenus par sa classe pour



chacune de ces compétences. Il peut aussi proposer de la remédiation ou de l'approfondissement à l'aide de sujets courts soumis et classés par ordre de pertinence en fonction des résultats du groupe.

RETOURS D'USAGES

Un projet eTwinning

Le projet européen *The eCity Challenge* concerne une classe de seconde, dont une partie en section européenne. Le parcours se déroule essentiellement en cours d'anglais mais aussi dans le cadre de l'enseignement Sciences Numériques et Technologie (SNT) pour certains aspects plus techniques comme la prise en main du *TwinSpace*. Les élèves partenaires vivent dans une ville virtuelle et ont comme défi d'organiser cette société, d'en établir et de faire respecter les règles. Le projet ayant lieu à distance, les notions de sécurité en ligne sont abordées, de même que les notions de démocratie participative, de sauvegarde de l'environnement et de relations intergénérationnelles.

Safer Internet Day

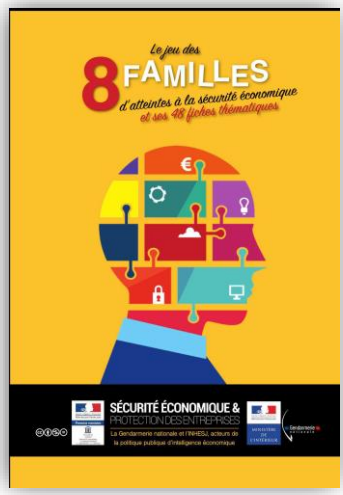
Au cours du projet eTwinning sont célébrées la journée européenne des langues ainsi que la journée internationale pour un Internet plus sûr ou *Safer Internet Day* (SID), l'une des actions (organisée chaque année au mois de février) du programme européen *Better Internet For Kids* initié par la Commission européenne.

Partant du constat que les enfants accèdent à Internet plus tôt, sur un plus grand nombre d'appareils, qu'ils jouent en ligne, utilisent des applications, et ce souvent sans la supervision d'un adulte, il est nécessaire d'envisager, au-delà des opportunités d'apprentissage, de communication, de créativité, que ces pratiques les exposent à des risques accrus. Cette journée – célébrée dans plus de 170 pays promeut un usage plus sûr et plus responsable

des technologies numériques par les jeunes usagers. Les modalités de participation à cette journée événement, ainsi que de nombreuses ressources (filtrage par types de ressources, thèmes et publics) sont à retrouver sur le site d'**Internet sans crainte**.

CONTENUS LUDIQUES

Jeu des 8 familles d'atteintes à la sécurité économique



L'**Institut des hautes études du ministère de l'Intérieur (IHEMI)** et la **Direction générale de la Gendarmerie nationale** proposent un livret de 48 fiches thématiques classées en 8 familles accompagnées d'un **jeu de cartes** : **les atteintes physiques sur site**, **les fragilisations/désorganisations d'entreprise**, **les atteintes aux savoir-faire**, **les intrusions**, **les risques financiers**, **les risques informatiques** (la destruction de données, vols d'ordinateurs et de supports de stockage, les intrusions dans les STAD, les attaques DDoS, la défiguration de site, les risques liés au BYOD), **les fragilités humaines** (l'ingénierie sociale, la pression ou menace sur client, la pression ou menace sur fournisseur, les dérives personnelles, l'absentéisme, la clause de confidentialité), **les atteintes à la réputation** (les attaques informationnelles, les attaques

sur l'identité de l'entreprise, l'usurpation d'identité, le respect de l'environnement, la protection des données personnelles, la responsabilité sociétale de l'entreprise).

CyberEnJeux

Le kit CyberEnJeux, élaboré par le **Laboratoire d'innovation publique** de l'**ANSSI** et le **ministère de l'Éducation nationale et de la Jeunesse**, avec le soutien de la communauté *Open Serious Game*, constitue un support pour la construction d'une séquence pédagogique[19] dédiée à la formation de leurs élèves à la cybersécurité par la conception de jeux. Une version 2 sera proposée en 2023. Quatre types de fiches sont mises à disposition : organisation, cybersécurité, jeux, objectifs pédagogiques.

Composé de **fiches thématiques** et **pédagogiques** ainsi que de **fiches pratiques** portant sur la cybersécurité, le kit **CyberEnJeux** est publié sous licence libre.

Suivant la même démarche ludique il faut rappeler l'existence du kit **123 Cyber** diffusé en 2019 et constitué d'un jeu de 35 cartes ainsi que d'un livret d'animation (diffusé en licence libre au format PDF sur GitHub).

Jeux d'évasion

Dans le cadre d'un scénario issu élaboré au cours des travaux académiques mutualisés, **TraAM EMI** (2020-21) **Sandrine Larrieu-Lacoste** (académie de Toulouse) invite les élèves à participer à un jeu pédagogique numérique, mixte et immersif, pour connaître les règles en matière d'hygiène et de cybersécurité tout en découvrant l'histoire des femmes scientifiques ayant contribué au développement de l'informatique : Grace Hopper, Ada Lovelace, Joan Clarke, Dorothy Vaughan, Aurélie

[19] L'académie de Toulouse publie un exemple d'expérimentation pédagogique

Jean. Cette activité baptisée « Le chronocrypteur » est menée au niveau de l'enseignement Sciences numériques et technologie. Elle s'appuie sur une application en ligne et un ensemble de cartes à imprimer.

Illustrations et design : Triton Mosquito © Inria

La séquence toulousaine est à rapprocher du jeu de cartes « 7 familles » distribué par l'Inria et ses partenaires visant à mettre en lumière 42 (+1) personnalités de l'histoire de l'informatique. La troisième famille est consacrée à la sécurité et à la confidentialité. Le jeu est disponible gratuitement en version papier sur simple demande mais peut être aussi téléchargé au format PDF.

CYBEReSCAPE est un jeu d'évasion pédagogique créé pour l'enseignement en SNT en classe de 2de, par **Mélanie Fenaert**. Ce scénario amène les élèves à prendre le rôle de jeunes recrues de la « Cyberacadémie », unité de formation d'agents spécialistes de la cybersécurité. Lors de leur première visite des locaux, le réseau de l'académie subit une cyberattaque. Les jeunes agents ont 45 minutes pour trouver comment contrer le *hackeur*.

Durant cet *escape game*, les élèves découvrent ou révisent différentes notions du programme de SNT : réseaux sociaux, cybersécurité, Web, Internet, données structurées. La mécanique du jeu d'évasion repose sur la collaboration et la coopération entre joueurs, et au final entre équipes. Après la phase de jeu, le *debriefing* permet de revenir sur les contenus disciplinaires et d'aller plus loin sur le sujet de la cybersécurité.

Le kit complet de la mise en œuvre du jeu et de ses éléments sont rassemblés dans un fichier compressé à télécharger sur le site de la **DANE de l'académie de Versailles**.

Les décodeuses du numérique

unDraw

L'**Institut des sciences de l'information et de leurs interactions (INS2I)** du CNRS publie sur son site en consultation libre la bande dessinée « Les décodeuses du numérique » crayonnée par la dessinatrice **Léa Castor**, ainsi que des ressources complémentaires, pour les classes, pour les enseignants et les élèves.

Extrait de la BD - Portrait de Caroline Fontaine p.25 ©CNRS Éditions

Ce support vise à « mettre en avant la diversité des recherches en sciences du numérique et contribuer à briser les stéréotypes qui dissuadent les femmes de s'engager dans cette voie ».

Pour en faciliter l'utilisation dans les lycées, en particulier en lien avec le programme de seconde en SNT, un livret d'accompagnement a été conçu ainsi que des fiches à destination des élèves.

Ces **fiches pédagogiques** structurées en trois catégories (*Les sciences du numérique et leur contexte*, *Notions transversales et applications*, *Les décodeuses et l'enseignement SNT*) sont également consultables sur **Folios** et **Étincel**.

Passe ton *Hack* d'abord

Co-organisé par le **Commandement de la cyberdéfense** (COMCYBER) et la **Direction générale de l'enseignement scolaire** (DGESCO) du ministère de l'Éducation nationale et de la Jeunesse, le jeu de « capture du drapeau » (*CTF*, capture the flag en anglais) « Passe ton Hack d'abord » initie les élèves (niveau seconde à BAC+2) à la cybersécurité en complément des programmes scolaires, et vise à stimuler leur intérêt pour ce domaine.

Le principe consiste à exploiter des vulnérabilités affectant des systèmes de manière à s'y introduire afin de récupérer les drapeaux, preuves de ladite intrusion. Le concours « Passe ton hack d'abord » comprend 15 épreuves accessibles en ligne portant sur les sujets de programmation, de réseau et de cryptographie.

L'EMI en bibliothèques

Ce kit sous licence Creative Commons proposé par **Bibliothèques sans frontières** contient 58 fiches d'activité et 43 ressources de compréhension classées en 3 grands thèmes : *Se protéger*, *Se représenter* et *S'informer en ligne*. Chaque thème est divisé en objectifs pédagogiques qui s'accompagnent d'activités et de ressources de compréhension.

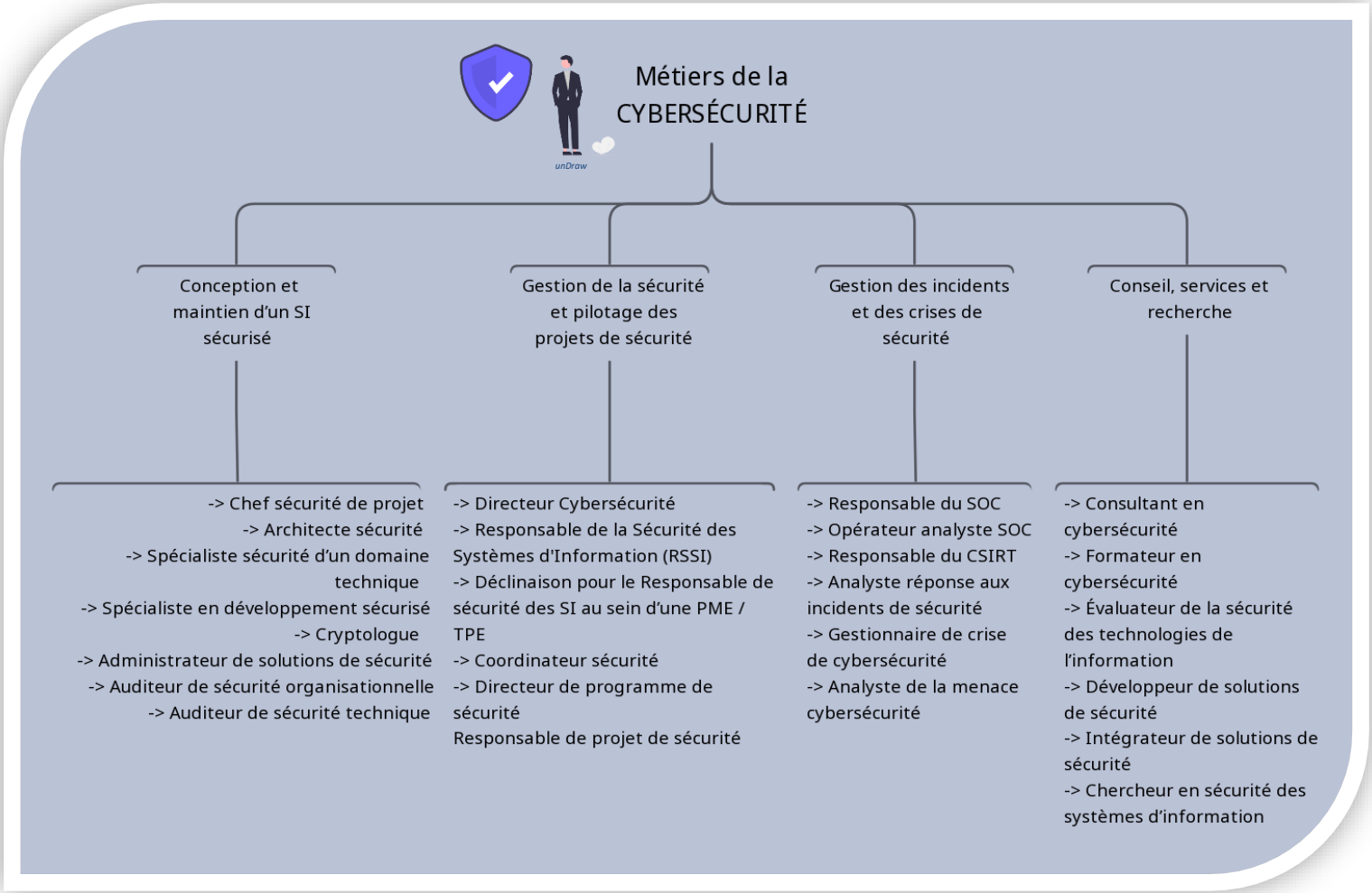
Exemple de fiche activité - CC

Le premier objectif d'autoprotection et de protection des autres contre les dangers possibles dans les environnements numériques comprend plus particulièrement des activités liées à la cybersécurité comme l'ingénierie sociale, notamment les attaques par harponnage ou hameçonnage (p.39-51) éventuellement ciblé, par SMS ou courrier électronique.

LES MÉTIERS DE LA CYBERSÉCURITÉ

L'ANSSI a mené en 2022 une enquête sur l'attractivité et la représentation des métiers de la cybersécurité, avec le soutien de la **délégation générale à l'emploi et à la formation professionnelle (DGEFP)** du ministère du Travail, du Plein Emploi et de l'Insertion, ainsi que de l'**Agence nationale pour la formation professionnelle des adultes (Afpa)**.

Elle propose également un panorama des métiers (édition 2020) comprenant deux parties. La partie principale, consacrée aux métiers dédiés à la cybersécurité (proposition de visualisation graphique ci-dessous), est organisée en 4 grandes familles et la seconde consacrée aux professions connexes.



Ces familles se retrouvent au sein du Campus Cyber, projet fédérateur initié par le Président de la République. Dans cet écosystème, le Groupe de Travail *Formation*

favorise la mutualisation de ressources au sein du Studio des communs. Les travaux ont abouti, parmi les **communs** produits, à la réalisation d'une Matrice de compétences des Métiers de la Cybersécurité, « outil d'aide à l'orientation, à l'insertion des jeunes diplômés et à la reconversion vers et au sein des métiers de la cybersécurité ».

SOURCES

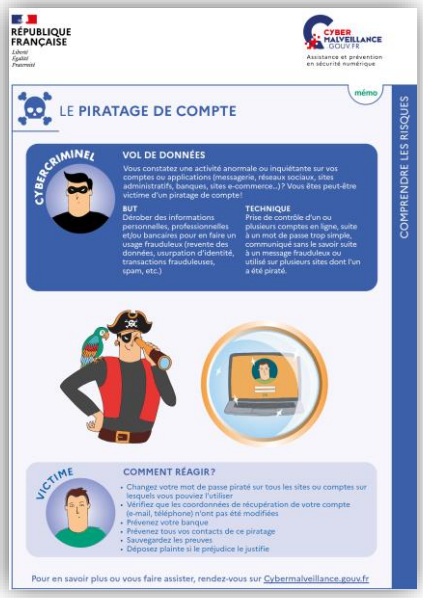
Enseigner

Le **portail national éduscol** consacre une page à des ressources de formation, des supports pour préparer des **séances** de sensibilisation et des propositions d'activités à mener en classe en lien avec les **programmes**.

La plateforme **Pix** d'évaluation, de développement et de certification des compétences numériques issues du référentiel **CRCN** (cadre de référence des compétences numériques, inspiré du cadre européen **DigComp**) propose notamment sur la compétence « Sécuriser l'environnement numérique » un contenu pédagogique expertisé (sélection de défis).

Se former

La plateforme de formation continue **M@gistère** met à disposition des enseignants, cadres et administratifs, un parcours libre de sensibilisation intitulé « Agir pour contribuer à ma sécurité numérique et à celle de mon organisation » et structuré en 3 modules : Module 1 (comprendre les menaces et les risques), Module 2 (agir en connaissant les bonnes pratiques), Module 3 (transmettre, pourquoi et comment sensibiliser). Ce parcours est conçu par le Groupement d'Intérêt Public Action contre la Cybermalveillance (GIP ACYMA).



Exemple de fiche mémo (Cybermalveillance)

Cybermalveillance.gouv.fr, dispositif national de sensibilisation, prévention et d'assistance aux victimes d'actes de cybermalveillance, offre à tous une liste de

supports variés (article, fiche réflexe, fiche mémo, fiche bonne pratique, vidéo de sensibilisation, test de connaissances) pour comprendre les cybermenaces et savoir comment y réagir, ainsi que des bonnes pratiques à adopter pour assurer sa sécurité numérique.

Le **cyber guide famille proposé par** Cybermalveillance.gouv.fr offre des bonnes pratiques. Il apporte des réponses concrètes à la nécessité de sensibiliser le grand public et notamment les familles : mots de passe, sauvegarde des données, mise à jour de sécurité, antivirus, achats en ligne, messages suspects, réseaux sociaux, Wi-Fi publics ou inconnus, objets connectés, cyberharcèlement[20].

Deux cours en ligne permettent en outre de s'initier à la cybersécurité, le **MOOC de l'ANSSI SecNum *académie*** composé de 4 modules (panorama de la SSI, sécurité des systèmes d'information, sécurité de l'authentification, sécurité sur Internet, sécurité du poste de travail et nomadisme) et le cours *Défis et enjeux de la cybersécurité* sur FUN structuré en 7 semaines (approche sociétale de la cybersécurité, cybersécurité pour le citoyen : la *Data Privacy* comme levier d'engagement, règles juridiques de la cybersécurité, introduction à la cybersécurité logicielle, attaques et défenses en intelligence artificielle, *Security Information and Event Management* (SIEM) dans la cyberdéfense, cybersécurité dans le monde réel : l'exemple des systèmes industriels).

L'atelier RGPD est une formation en ligne gratuite, illimitée et ouverte à tous proposée par la CNIL. Elle permet de sensibiliser les professionnels à la protection des données et d'accompagner leur mise en conformité.

Enfin, L'académie de Versailles produit dans le cadre de sa campagne de sensibilisation à la cybersécurité, des bandes dessinées à destination de sa communauté éducative, une série d'audios de culture numérique (dont trois en lien avec la

[20] Voir également le jeu de cartes de la CNIL « Prudence sur Internet »

cybersécurité, les *cookies*, le RGPD et le mot de passe) ainsi qu'un livret de 7 préconisations et une étude concrète de cas (usurpation d'identité sur un ENT).

Se mettre en veille

Le salon public de discussion thématique TCHAP « Cybersécurité et éducation » est ouvert sur la messagerie de l'État *Tchap* : il permet d'échanger et de partager des ressources avec la communauté d'enseignants et de professionnels de la cybersécurité.

Le « Panorama de la cybermenace 2022 » publié par l'ANSSI dresse un état des grandes tendances des actions malveillantes et des activités cybercriminelles comme l'espionnage informatique, les intrusions, les rançongiciels, les services de vente d'accès ou de programme malveillant à la demande, etc.

Pour suivre l'actualité le compte Twitter @ANSSI_FR est un outil précieux. Le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) est aussi « une des composantes curatives complémentaires des actions préventives assurées par l'ANSSI ». Il publie des alertes de sécurité, des rapports des menaces et des incidents, des avis de sécurité, des indicateurs de compromission, des recommandations et des bulletins d'actualité. Le compte officiel Twitter @cybervictimes du dispositif national Cybermalveillance constitue une ressource tout aussi importante et accessible pour un plus large public.

Suivre la recherche

Carnet Hypotheses

Le Carnet Éducation, numérique et recherche assure une veille sur la plateforme **Hypotheses** de carnets de recherche en sciences humaines et sociales et valorise des travaux de recherche soutenus par la Direction du numérique pour l'éducation (Ministère de l'Éducation nationale et de la Jeunesse).

Décryptage de séries télévisées

Le projet Demoseries, financé par le **Conseil Européen de la Recherce** (CER) et hébergé par l'**Université Paris 1 Panthéon-Sorbonne**, rassemble une équipe de philosophes, sociologues et politologues qui explorent un corpus de « séries télévisées de sécurité »,

considérées comme outil d'éducation politique et moral. Une partie des réflexions est consacrée aux questions de cybersécurité, par exemple dans la série *Black Mirror*.

Informatique quantique

Dans ce registre à dimension prospective on peut également s'intéresser au projet international PROMETHEUS ayant « pour objectif de fournir, d'ici 2030, aux communautés académiques, industrielles et étatiques des outils cryptographiques post-quantiques sûrs et opérationnels ». Potentiellement les ordinateurs quantiques de demain, en raison de leur puissance de calcul et de traitement des données, seraient en capacité de déchiffrer des informations sensibles, dans le cadre d'une démarche du « stocker maintenant, déchiffrer plus tard » précise **Sébastien Canard**[21].

Références

- ANSSI. Guide d'hygiène informatique (2017)
- ANSSI – DINSIC. Agilité et sécurité numériques (2018)
- République française – Légifrance. LOI n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public (2022)

[21] Audio du *Monde Numérique* : https://www.mondenumerique.info/nous-developpons-les-standards-cryptographiques-du-futur-sebastien-canard-orange

- ANSSI. Guide attaques par rançongiciel, tous concernés (2020)
- Cybermalveillance. Dispositif national d'assistance aux victimes d'actes de cybermalveillance, de prévention et sensibilisation aux risques numériques et d'observation de la menace
- DINUM. Référentiel général d'écoconception de services numériques (2022)
- MiNumEco. Guide de bonnes pratiques numérique responsable pour les organisations (2022)
- Designers éthiques. Le guide d'écoconception de services numériques (2022)
- CNIL. La sécurité des données personnelles (2018)
- CNIL. La forme des choix : données personnelles, design et frictions désirables (2019)
- Canopé. Les données à caractère personnel (2018)
- Campus Cyber : Wiki du Studio des Communs (2022)

Lettre ÉduNum proposée par la direction du numérique pour l'éducation
Bureau de l'accompagnement des usages et de l'expérience utilisateur (DNE-TN3)

✉ **Contact courriel**

Vous recevez cette lettre car vous êtes abonné à la lettre ÉduNum thématique

Souhaitez-vous continuer à recevoir la lettre ÉduNum thématique ?

Abonnement / Désabonnement

À tout moment, vous disposez d'un droit d'accès, de modification, de rectification et de suppression des données qui vous concernent (art. 34 de la loi Informatique et Libertés du 6 janvier 1978). Pour consulter nos mentions légales, cliquez ici.