NUMÉRIQUE ET CYBERSÉCURITÉ

PROGRAMMES DE L'ÉCOLE ET DU COLLÈGE

LE SOCLE COMMUN DE CONNAISSANCES, DE COMPÉTENCES ET DE CULTURE

Le socle commun entré en vigueur à la rentrée 2016 donne une place nouvelle aux langages informatiques. Le domaine « Des langages pour penser et communiquer » recouvre quatre types de langages, parmi lesquels les langages mathématiques, scientifiques et informatiques.

À L'ÉCOLE ÉLÉMENTAIRE ET EN CLASSE DE 6e (CYCLES 2 ET 3)

Le programme d'enseignement moral et civique (EMC) prévoit un travail sur la responsabilisation à l'usage du numérique.

Dès le cycle 2 :

> *Le développement des aptitudes au discernement et à la réflexion critique prend appui sur l'éducation aux médias et à l'information ;*

Le programme du cycle 3 précise par ailleurs que :

> *Dès lors qu'ils disposent d'un accès individuel aux outils numériques de l'école et l'établissement, les élèves sont invités à utiliser le numérique de manière responsable (…) . Ils sont sensibilisés aux enjeux et aux dangers relatifs à l'usage des réseaux sociaux.*

Si l'éducation aux médias et à l'information (EMI) ne fait pas l'objet d'un enseignement spécifique comme au cycle 4, elle figure dans les programmes des cycles 2 et 3. Le Conseil supérieur des programmes a formulé des orientations pour l'EMI dans ces deux cycles. Les questions relatives aux droits et responsabilités dans l'usage du numérique, aux risques et aux traces laissées par les activités en ligne y tiennent une place particulière.

AU CYCLE 4 (5e-4e-3e)

Au cycle 4, les notions d'algorithmique et de programmation sont traitées conjointement dans les programmes de mathématiques et de technologie, dans lesquels elles constituent un thème à part entière. Les élèves doivent connaître les

notions de séquences d'instructions, de boucles, d'instructions conditionnelles. En technologie, « les élèves utilisent des outils numériques et conçoivent tout ou partie d'un programme, le compilent et l'exécutent pour répondre au besoin du système et des fonctions à réaliser ».

Les élèves apprennent également à « devenir des usagers des médias et d'Internet conscients de leurs droits et devoirs et maitrisant leur identité numérique ».

L'éducation aux médias et à l'information, présente dans tous les champs du savoir transmis aux élèves et prise en charge par tous les enseignements, aide à maîtriser les systèmes d'information et de communication. Elle initie à des notions comme celles d'identité et de trace numériques « dont la maîtrise sous-tend des pratiques responsables d'information et de communication ». En EMC, « l'identité numérique » est étudiée comme composante de l'identité personnelle et légale. « Le harcèlement sur Internet et les réseaux sociaux » est également un objet d'enseignement.

PROGRAMMES DU LYCÉE GÉNÉRAL ET TECHNOLOGIQUE

De nouveaux programmes pour le lycée général et technologique ont été publiés en 2019. Plusieurs enseignements mettent l'accent sur les questions liées au numérique et à la cybersécurité.

SCIENCES NUMÉRIQUES ET TECHNOLOGIE (ENSEIGNEMENT DE TRONC COMMUN - SECONDE)

Cet enseignement a pour objet de permettre d'appréhender les principaux concepts des sciences numériques mais également de permettre aux élèves de comprendre le poids croissant du numérique et les enjeux qui en découlent. Dans la partie « Le Web », la sécurité et la confidentialité sont traitées :

> *En formulant des requêtes sur des sites Web dynamiques et en laissant des programmes s'exécuter sur sa machine, l'utilisateur prend des risques : il peut communiquer des informations personnelles à son insu à des serveurs qui en gardent une trace, à distance ou localement par des cookies, ou encore charger des pages contenant des programmes malveillants, par exemple permettant d'espionner en continu les actions de l'utilisateur. Par ailleurs, un navigateur peut garder un historique de toutes les interactions, et le laisser accessible aux sites connectés. L'utilisateur peut utiliser des services qui s'engagent à ne pas garder de traces de ses interactions, par exemple certains moteurs de recherche. Il peut aussi paramétrer son navigateur de façon à ce que celui-ci n'enregistre pas d'historique des interactions. De fausses pages peuvent encore être utilisées pour l'hameçonnage des utilisateurs. Un nom de lien pouvant cacher une adresse Web malveillante, il faut examiner cette adresse avant de l'activer par un clic.*

NUMÉRIQUE ET SCIENCES INFORMATIQUES (ENSEIGNEMENT DE SPÉCIALITÉ – PREMIÈRE ET TERMINALE GÉNÉRALES)

Cet enseignement a vocation à développer plusieurs compétences, parmi lesquelles « faire un usage responsable et critique de l'informatique ». Une partie du programme est dédiée aux interactions entre l'homme et la machine sur le Web.

ENSEIGNEMENT MORAL ET CIVIQUE (ENSEIGNEMENT DE TRONC COMMUN)

L'axe 2 du programme de seconde, « Garantir les libertés, étendre les libertés : les libertés en débat » proposent plusieurs objets d'enseignement parmi lesquels « Les flux informationnels et leur régulation sur internet » ; « les données numériques, traitement et protection (règlement général sur la protection des données) ».

En classe terminale, le thème annuel est « La démocratie, les démocraties » et la cybersécurité est explicitement évoquée dans l'axe 1 : « Fondements et expériences de la démocratie » : « La protection des démocraties : sécurité et défense nationales ; lutte contre le terrorisme ; état d'urgence et législation d'exception ; cybersécurité ».

SÉRIE STMG

Certains enseignements de la voie technologique accordent aussi une importance particulière à la question de la cybersécurité.

SCIENCES DE GESTION ET NUMÉRIQUE

En classe de première, cet enseignement comporte un thème intitulé « Numérique et intelligence collective » : « L'étude du thème vise à appréhender les contributions du numérique aux divers processus de l'entreprise (gestion, production, logistique, etc.) et à mettre en évidence les opportunités et les risques qu'il génère. »

SYSTÈME D'INFORMATION ET DE GESTION

La cybersécurité est un objet d'enseignement dans cette spécialité de la série STMG, où le programme précise : « La sécurité des systèmes d'information s'étend à la cybersécurité pour prendre en compte les évènements issus du cyberespace qui sont susceptibles de compromettre la disponibilité, l'intégrité, la confidentialité ou la traçabilité des données. Cela consiste, pour l'organisation, à prévenir les actes de malveillance délibérés ou la négligence avec intention de nuire ; cela exige des techniques nouvelles comme la mise en place d'une cyberdéfense pour lutter contre la cybercriminalité. Les données font l'objet d'une protection élevée, conformément aux obligations en la matière et aux avantages stratégiques et économiques qu'elles peuvent représenter. »

SÉRIE STI2D

En STI2D, CyberEnJeux peut être un support connexe pour introduire une dimension de sécurité numérique lors de projets thématiques en particuliers avec les objets connectés et des thèmes des programmes (santé, efficacité énergétique, habitat de demain, ville du futur).

ENSEIGNEMENT OPTIONNEL DE DROIT ET GRANDS ENJEUX DU MONDE CONTEMPORAIN

Dans cette option proposée en classe terminale, une partie du programme s'intitule « Intelligence artificielle et justice » laquelle comporte un questionnement sur « Comment le droit peut-il appréhender la cybercriminalité ? ». Le programme indique par la suite que « des groupes de pirates informatiques créent des programmes malveillants à des fins criminelles spécifiques – on nomme ce phénomène « cybercriminalité ». Virus informatiques et chevaux de Troie sont ainsi capables de dérober des codes d'accès de comptes bancaires, de promouvoir des produits ou services sur les ordinateurs de leurs victimes, d'utiliser illégalement les ressources des ordinateurs infectés afin de développer et de lancer des campagnes de pourriels (spams), des attaques contre des réseaux distribués ou des opérations de chantage. Prolongement possible – débat : une banque victime d'une cyberattaque est-elle responsable vis-à-vis de ses clients dont les données ont été dérobées et les comptes bancaires vidés ? »

PROGRAMMES DU LYCÉE PROFESSIONNEL

De nouveaux programmes ont été publiés pour le lycée professionnel en 2019 et 2020. Plusieurs enseignements mettent l'accent sur les questions liées au numérique et à la cybersécurité.

ÉCONOMIE-GESTION AU LYCÉE PROFESSIONNEL

En CAP, dans le module sur les mutations de la relation de travail, le programme précise que « L'usage régulier de l'e-communication questionne le périmètre de son utilisation : à des fins personnelles ou professionnelles, sur le lieu de travail ou ailleurs. Il permet de poser la question du décloisonnement entre la vie privée et la vie publique et celle de l'identité numérique ».

En baccalauréat professionnel, dans le module 2 « La consommation : quels choix pour les ménages ? » les élèves sont amenés à « repérer l'influence du numérique dans l'évolution des modes de consommation ». Par exemple, le professeur peut montrer que « la consommation responsable prend en compte de nouveaux critères, notamment le respect de l'environnement, l'économie locale, la santé… ». Les élèves seront également amenés à savoir « Comment protéger le consommateur dans son acte d'achat ? », par exemple pour le e-commerce, l'élève s'interroge sur le traitement et l'utilisation des données personnelles collectées.

SYSTÈMES NUMÉRIQUES EN PARTICULIER RÉSEAUX INFORMATIQUES ET SYSTÈMES COMMUNICANTS

Un point d'entrée pour initier une réflexion intégrant la sécurité numérique dans le cadre de la compréhension des réseaux, l'intégration de matériels communicants et d'objets connectés.

ENSEIGNEMENT MORAL ET CIVIQUE

La question du numérique est plus particulièrement abordée dans le thème dédié à la liberté (« La Liberté, nos libertés, ma liberté » en classe de seconde professionnelle). En classe de première, dans le second thème « Préserver la paix et protéger des valeurs communes » sont abordées la défense et sécurité en France et en Europe. Pour exemple, « Face aux attentats terroristes, l'État se dote de nouveaux dispositifs et outils, de nouvelles instances de sécurité et de renseignement, y compris dans le domaine de la cybersécurité. »

En classe terminale dans le thème annuel « S'engager et débattre en démocratie autour des défis de société » est abordé « La digitalisation présente des risques pour les libertés et la sécurité des États et des individus. » Le programme précise qu'il est possible de faire référence, par exemple, « à la loi relative à l'informatique, aux fichiers et aux libertés (1978), à la création de l'Agence nationale de la sécurité des systèmes d'information (2009) et à la loi pour une république numérique (2016). »

FRANÇAIS

Dans le préambule du programme de la classe de première, il est précisé :

> *Enseigner le français à l'heure du numérique : le français prend sa part dans l'apprentissage des pratiques numériques comme dans la réflexion sur leurs enjeux. […] Le français concourt ainsi à l'acquisition d'attitudes et de capacités fondamentales dans l'univers numérique : identifier des sources et vérifier leur fiabilité ; trier, hiérarchiser et rédiger des informations pertinentes ; adopter une attitude responsable ; collaborer en réseau ; élaborer des contenus numériques…*

Dans celui de la classe terminale, pour la même pratique, il est précisé à ce sujet que les élèves doivent être capables de :

> *Se repérer dans les sources ; trier, hiérarchiser et rédiger des informations pertinentes ; adopter une attitude responsable vis-à-vis d'elles ; adapter sa lecture au support, comme son message aux destinataires.*

ÉVALUATION DES COMPÉTENCES NUMÉRIQUES

Pour suivre l'acquisition des compétences numériques et mesurer le niveau de maîtrise de chaque élève, étudiant ou professionnel, les ministères chargés de l'éducation nationale et de l'enseignement supérieur ont élaboré un cadre de référence des compétences numériques (décret n° 2019-919 du 30 août 2019). Une certification nationale est délivrée à tous les élèves par le groupement d'intérêt « PIX » en fin de cycle 4 et du cycle terminal.

Ce travail s'inscrit dans la démarche du référentiel des compétences numériques élaboré par la Commission européenne (DIGCOMP). Il comprend seize compétences organisées dans cinq domaines spécifiques :

- information et données ;
- communication et collaboration ;
- création de contenu ;
- protection et sécurité ;
- environnement numérique.

Le domaine « protection et sécurité » se décline de la façon suivante :

4.1. Sécuriser l'environnement numérique	Sécuriser les équipements, les communications et les données pour se prémunir contre les attaques, pièges, désagréments et incidents susceptibles de nuire au bon fonctionnement des matériels, logiciels, sites internet, et de compromettre les transactions et les données (avec des logiciels de protection, la maîtrise de bonnes pratiques…).
4.2. Protéger les données personnelles et la vie privée	Maîtriser ses traces et gérer les données personnelles pour protéger sa vie privée et celle des autres, et adopter une pratique éclairée (avec le paramétrage des paramètres de confidentialité, la surveillance régulière de ses traces…).
4.3. Protéger la santé, le bien-être et l'environnement	Prévenir et limiter les risques générés par le numérique sur la santé, le bien-être et l'environnement mais aussi tirer parti de ses potentialités pour favoriser le développement personnel, le soin, l'inclusion dans la société et la qualité des conditions de vie, pour soi et pour les autres (avec la connaissance des effets du numérique sur la santé physique et psychique et sur l'environnement, et des pratiques, services et outils numériques dédiés au bien-être, à la santé, à l'accessibilité…).