# Manuel CYBER.VET.EU

## Améliorer la préparation à la cybersécurité de l'enseignement et de la formation professionnels européens. et de la formation et de la formation professionnelle


2020-1-DE02-KA226-VET-008327

TANDEM PLUS NETWORK avec le consortium de CYBER.VET.EU :

Co-funded by the
Erasmus+ Programme
of the European Union

Ce projet a été cofinancé avec le soutien de la Commission européenne. 2020-1-DE02-KA226-VET-008327

# Sommaire

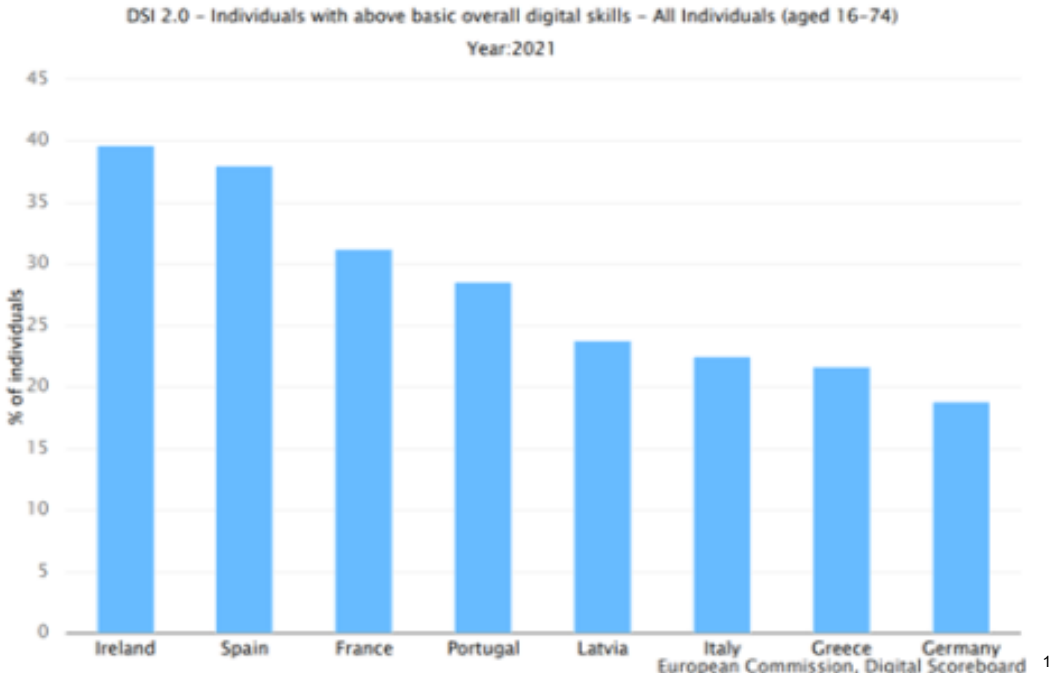


## a) La mise en œuvre du projet CYBER.EU.VET

L'Union européenne est confrontée à un défi de taille représenté par la pandémie de Covid-19. De nombreux secteurs sont fortement touchés par ces crises et l'éducation en fait certainement partie.

De plus en plus d'utilisateurs sont aujourd'hui contraints d'utiliser des cours ou des formations en ligne. Il est donc plus important que jamais de reconnaître les menaces quotidiennes qui pèsent sur notre sécurité. Ce sujet est également reconnu comme fondamental par la

Commission européenne qui organise chaque année un mois européen de la cybersécurité, dont le site web comprend déjà du matériel éducatif et des campagnes de sensibilisation spécifiques comme la campagne "Get cyber skilled" en 2018.
Le projet CYBER.EU. VET comprend 8 partenaires (ONG NEST - Allemagne (LEADER), MEATH COMMUNITY RURAL AND SOCIAL DEVELOPMENT PARTNERSHIP LIMITED - Irlande, TANDEM PLUS - Un réseau européen basé en France, COFAC COOPERATIVA DE FORMACAO E ANIMACAO CULTURAL CRL- Portugal, LATVIJAS ASOCIACIJA EIROPAS KOPIENAS STUDIJAM - Lettonie, ASOCIACIÓN EDUCATIVA POR LA INTEGRACIÓN Y LA IGUALDAD - Espagne, INECIA DIGITAL - Espagne, Extrafondente Open Source - Italie).



[1]

L'objectif principal de CYBER.EU.VET est de renforcer la capacité de l'EFP européen à reconnaître et à gérer les menaces de cybersécurité (par exemple, les attaques de phishing, les botnets, les fraudes financières et bancaires, les fraudes de données) dans un contexte historique où la formation en ligne est de plus en plus utilisée.

[1] Profil d'indicateurs de l'ESMS (ESMS-IP) Agence de compilation : Eurostat, l'office statistique de l'Union européenne.

### i. Impact du projet:

Le projet a eu un impact aux niveaux local, régional et national en impliquant différents niveaux de parties prenantes, en proposant des solutions adaptées aux demandes des niveaux locaux, mais alignées à un niveau plus élevé, en développant, grâce au partenariat, du matériel de formation et des normes applicables à l'échelle européenne.
En particulier, l'impact sur les participants directs et les principaux groupes cibles a été le suivant :
- Les éducateurs de l'EFP - une capacité d'enseignement renforcée, ajoutant à leurs compétences une connaissance des principales menaces de sécurité numérique.
- Les éducateurs de l'EFP et les étudiants : des compétences numériques améliorées grâce au matériel de formation.
- Les éducateurs de l'EFP et les étudiants : une sensibilisation accrue aux menaces et à leurs risques réels, tant économiques que sociaux.
- Les établissements d'EFP seront mieux préparés à faire face aux risques de cybersécurité grâce aux outils CYBER.VET.EU, tant pour leurs éducateurs que pour leurs étudiants.

### ii. Personnes cibles

Le projet devrait avoir un impact positif et à long terme sur les différentes parties prenantes impliquées dans le projet, en particulier :

- les étudiants en EFP

- les experts en cybersécurité bénévoles

- les réseaux d'établissements d'EFP

- décideurs politiques.

### iii. Objectifs du projet CYBER.EU.VET:

- Le premier objectif spécifique sera de mieux préparer les enseignants de l'EFP à la gestion des menaces de cybersécurité, étant donné leur rôle central dans le transfert de connaissances des bonnes pratiques et des compétences à leurs étudiants.

- Le deuxième objectif spécifique est de sensibiliser les enseignants de l'EFP, les étudiants et leurs familles à l'importance de reconnaître ces risques quotidiens, qui peuvent avoir un impact économique et social sur tous les citoyens européens.
- Le troisième objectif spécifique est de soutenir les institutions publiques et les établissements d'enseignement et de formation professionnels pour qu'ils soient mieux préparés à faire face à ce type de défis, en leur fournissant des lignes directrices pour les mises en œuvre futures.

### iv. Produits intellectuels:

- P1: Analyse de la recherche : principaux défis et meilleures pratiques en matière de cybersécurité (partenaire responsable : ONG NEST BERLIN EV - E10166639)
- Matériel de formation de sensibilisation à la cybersécurité pour le secteur de l'EFP (partenaire responsable : INERCIA DIGITAL SL (E10145080)
- P3: Boîte à outils pour la formation des formateurs (partenaire responsable INERCIA DIGITAL SL (E10145080)
- P4: Le manuel de cybersécurité pour les établissements d'enseignement et de formation professionnels : meilleures pratiques, matériel de formation et lignes directrices pour de futures mises en œuvre (partenaire responsable TANDEM PLUS - E10103913).

Parallèlement au développement des résultats intellectuels, l'autre objectif du projet est de diffuser nos résultats dans toute l'UE auprès des participants potentiels, des multiplicateurs et des parties prenantes intéressées, afin de renforcer l'impact et la pertinence de CYBER.EU.VET.

### v. Qu'est-ce que la cybersécurité ?

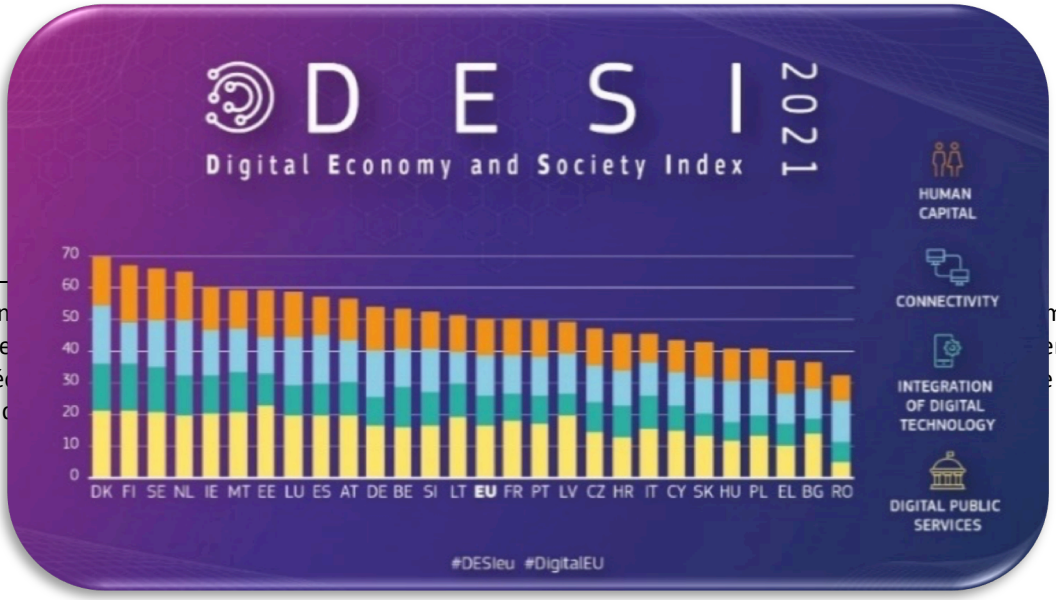
La définition officielle dans le droit européen se trouve dans le texte de la loi européenne sur la **cybersécurité**, où on entend par ce fenomène: "*on entend par cybersécurité les activités nécessaires pour protéger les systèmes de réseaux et d'information, les utilisateurs de ces systèmes et les*

*autres personnes concernées par les cybermenaces*" (art. 2.1)[2] :

Le droit communautaire, tout en adoptant l'approche de la "protection des systèmes de réseaux et d'information", souligne également que la cybersécurité protège non seulement les systèmes d'information, mais aussi (et peut-être surtout) les personnes, qu'il s'agisse d'utilisateurs de ces systèmes ou de tiers affectés de quelque manière que ce soit par les cybermenaces.

En décembre 2020, la Commission européenne et le Service européen d'action extérieure (SEAE) ont présenté une nouvelle stratégie de cybersécurité de l'UE visant à renforcer la résilience aux cybermenaces et à faire en sorte que les citoyens et les entreprises bénéficient de technologies numériques dignes de confiance.

Le Règlement (UE) 2021/887 établissant le centre de compétence européen en matière de cybersécurité industrielle, technologique et de recherche et le réseau des centres de coordination nationaux crée le centre de compétence européen en matière de cybersécurité (CCCE) et le réseau des centres nationaux de coordination (le "réseau") établit des règles pour les centres nationaux de coordination (CCN) et pour la création de la communauté de compétence en matière de cybersécurité.
Le Centre européen de compétences en cybersécurité aide l'UE à renforcer son leadership en matière de cybersécurité en améliorant la confiance et la sécurité, y compris la confidentialité, l'intégrité et l'accessibilité des données ; soutenir la résilience et la fiabilité des réseaux et des systèmes d'information, y compris les infrastructures critiques et les matériels et logiciels




[2] Règlemen… …mpétence européen e… …en en matière de cybersé… …e centres nationaux d…

couramment utilisés.

### vi. Principal défi en matière de compétences numériques en Europe

- Environ 70 millions d'Européens ne possèdent pas de compétences suffisantes en lecture, en écriture et en calcul.
- 24 % de la population de l'UE n'a pas de diplôme de l'enseignement secondaire supérieur
- 13 % des Européens n'ont jamais utilisé l'internet
- 43 % de la population de l'UE et 35 % de la main-d'œuvre de l'UE ont des compétences numériques insuffisantes.
- 42 % des personnes sans compétences numériques sont au chômage.
- Digital natives ≠ compétence numérique[3]

### vii. Contexte

Plus de 70 % des entreprises ont déclaré que le manque de personnel possédant des compétences numériques adéquates constitue un obstacle à l'investissement. L'Europe est également confrontée à une pénurie d'experts numériques capables de développer des technologies de pointe au profit de tous les citoyens.

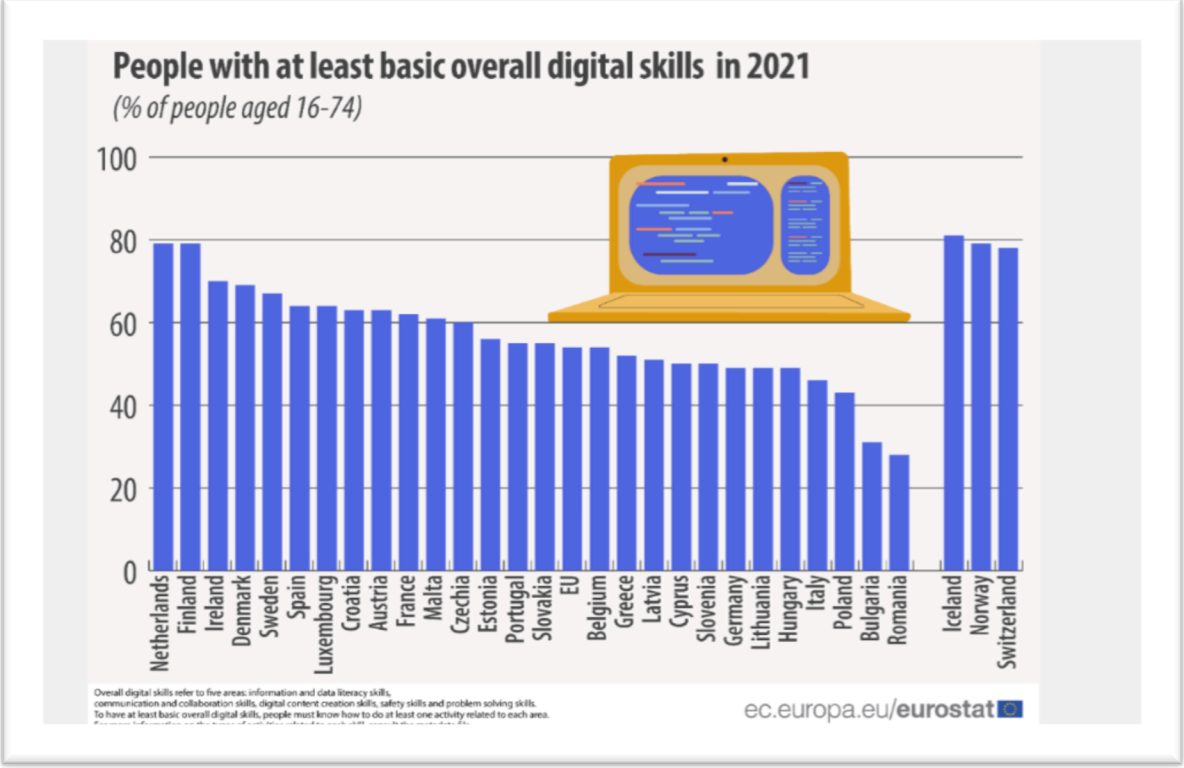
Une économie numérique forte, alimentée par des Européens possédant des compétences numériques, est essentielle pour l'innovation, la croissance, l'emploi et la compétitivité européenne. La diffusion des technologies numériques a un impact massif sur le marché du travail et le type de compétences nécessaires dans l'économie et la société. Les États membres, les entreprises, les prestataires de formation, la Commission européenne et d'autres organisations doivent travailler ensemble pour combler le déficit de compétences numériques. Pour suivre l'évolution de la transition numérique et du déficit de compétences numériques, la Commission publie chaque année l'indicateur des compétences numériques (DESI). Il permet de suivre les performances numériques des États membres dans différents domaines afin de contrôler les progrès réalisés et de déterminer les domaines dans lesquels des efforts supplémentaires sont nécessaires.

[3] Références : Rapport DESI 2018 – Capital humain ; 2017 Moniteur d'éducation et de formation, 2016 Communication sur les compétences, ICILS 2013.

En 2021, 54 % des personnes âgées de 16 à 74 ans dans l'UE disposaient au moins de compétences numériques générales de base.

En 2021, la proportion de personnes âgées de 16 à 74 ans ayant au moins des compétences numériques générales de base était la plus élevée aux Pays-Bas et en Finlande (79 % chacun), suivis de l'Irlande (70 %). En revanche, la part la plus faible était enregistrée en Roumanie (28 %), suivie de la Bulgarie (31 %) et de la Pologne (43 %).

Les indicateurs de compétences numériques font partie des indicateurs de performance clés dans le cadre de la Décennie numérique, qui définit la vision de l'UE en matière de transformation numérique. La boussole numérique fixe comme objectif que 80 % des citoyens de l'UE âgés de 16 à 74 ans possèdent au moins des compétences numériques de base d'ici 2030.




***Retour au sommaire ☐***

## b) Compétences numériques des éducateurs de l'EFP - un aperçu du consortium

### i. Allemagne:

- Rapport des données de l'EFP (2019) élaboré par l'Institut fédéral allemand pour l'enseignement et la formation professionnels (BIBB) a déclaré que "La numérisation va renforcer les changements structurels du marché du travail", se dirigeant vers un besoin de changement dans les capacités de formation dans les domaines respectifs.
  Comme le souligne la Résolution de la Conférence permanente des ministres de l'éducation et des affaires culturelles (2016-2017) le domaine de l'enseignement professionnel, la promotion des compétences liées à l'emploi dans le contexte du travail numérique et des processus commerciaux est une partie essentielle de la compétence des enseignants comme point de départ de leurs activités didactiques.

### ii. Irlande:

- L'une des principales stratégies de l'Irlande concernant les compétences numériques des éducateurs de l'EFP est la stratégie numérique nationale qui a été lancée en juillet 2013. Cette stratégie met l'accent sur l'engagement numérique et souligne comment l'Irlande peut bénéficier d'une société engagée numériquement.
  En ce qui concerne les compétences numériques des éducateurs de l'EFP, les preuves continuent de souligner qu'il existe un fossé croissant entre les éducateurs qui utilisent des appareils numériques dans leur classe comme outil d'apprentissage et ceux qui ne le font pas.

### iii. Portugal:

- Le système national de qualifications a réorganisé l'EFP en un système unique dans lequel les programmes conduisent à une double certification. L'EFP pour les adultes fait partie intégrante du système national de qualification, dont les éléments clés sont les programmes d'éducation et de formation pour adultes et la reconnaissance et la validation des acquis. Le Portugal a fait des progrès significatifs en ce qui concerne le niveau d'éducation, mais il reste inférieur à la moyenne de l'UE. Bien que moins qu'en

2015 (73,7 %), en 2019, la part des personnes ayant un faible niveau ou aucune qualification était de 50,2 %, la plus élevée de l'UE.

### iv. Italie:

- Dans le domaine de l'éducation, les actions ont été menées principalement par la mise en œuvre du plan national pour l'école numérique. Les directives du ministère de l'éducation, de l'université et de la recherche ont lancé une stratégie d'innovation globale pour l'école italienne et pour un nouveau positionnement de son système éducatif dans l'ère numérique. La plupart des actions de formation du personnel scolaire ont été destinées aux écoles primaires et secondaires, qui représentent la majorité des écoles en Italie, tandis qu'une faible attention a été accordée au secteur de l'enseignement et de la formation professionnels (EFP).

### v. Espagne:

- L'Agenda numérique pour l'Espagne (ADpE, Agenda Digital para España) publié en 2013, est la feuille de route pour la réalisation des objectifs fixés par l'Agenda numérique pour l'Europe en 2015 et 2020, ainsi que la réalisation d'objectifs spécifiques pour le développement de l'économie et de la société numérique en Espagne. Il s'articule autour de six grands objectifs et de plusieurs plans spécifiques. Le sixième objectif concerne la promotion de l'inclusion et de l'alphabétisation numériques et la formation de nouveaux professionnels des TIC.

### vi. France

- Si l'on observe le rythme des formations à l'utilisation des TIC dans les universités françaises qui les proposent, on constate qu'il n'existe pas de politique claire et durable de formation des formateurs à l'utilisation des TIC/E. Environ 58% ne déclarent qu'une seule session de formation par an, contre 7,4% par mois et 0,5% par semaine.
  Les statistiques montrent que la densité de la formation en informatique varie d'une région francophone à l'autre. Il y a plusieurs raisons à cela, dont les plus importantes sont sans doute liées aux institutions académiques et à leurs gouvernements.

### vii. Lettonie

- En 2020, le ministère de l'éducation et des sciences de la République de Lettonie a fait de l'amélioration de la compétence numérique des éducateurs un objectif prioritaire de la compétence professionnelle, en allouant à cette fin un financement supplémentaire (0,5 million EUR). La nécessité de sensibiliser les apprenants et les éducateurs à la sécurité des informations, à la protection de la vie privée et à l'utilisation de services électroniques fiables (stratégie de cybersécurité 2019-2022, domaine d'action "Sensibilisation du public, éducation et recherche").

### viii. Grèce

- Bien que l'acquisition de compétences numériques soit une composante qui ne devrait pas être absente de la boîte à outils éducative des éducateurs de l'EFP, une lacune importante peut être identifiée en surveillant le système éducatif actuel en Grèce. Malgré les nombreuses réformes des programmes d'enseignement, il apparaît que les éducateurs ne sont pas suffisamment équipés en connaissances en matière de TIC et manquent donc d'outils et de techniques pédagogiques axés sur le numérique qui pourraient améliorer le processus d'enseignement (ministère de l'éducation, 2019).

## *Conclusions*

Les recherches menées pour le projet CYBER.EU.VET ont révélé un manque de données et d'informations sur les compétences et les défis en matière de cybersécurité des éducateurs des établissements d'enseignement au niveau européen, ainsi qu'un nombre limité d'initiatives axées sur les questions de cybersécurité dans l'EFP, ce qui indique que le projet CYBER.EU.VET a abordé le sujet émergent dans tous les États membres. Actuellement, la plupart des activités et des projets se concentrent sur la sensibilisation à la cybersécurité de la population générale et sur l'amélioration des compétences numériques globales des éducateurs, ce qui a été influencé par l'adaptation rapide au processus de travail/apprentissage à distance.

Le consortium de partenaires présente de multiples facettes et est l'expression claire d'un degré différent de compétences numériques en Europe. Toutefois, indépendamment du classement DESI des différents pays, ce rapport de recherche du consortium peut être utilisé pour tirer des indications significatives et valables pour l'ensemble du contexte européen. Le sentiment d'un besoin de formation est clair, même parmi les enseignants de l'EFP qui ont

déjà été formés aux TIC. Il n'y a pas de rejet de la nécessité de la formation, ni de remise en cause de son utilité. On constate également que plus les enseignants se sentent exposés à des risques psychosociaux, éthiques, juridiques, techniques ou sanitaires, plus ils disent ressentir un besoin de formation. Selon une enquête nationale, plus de la moitié des enseignants qui se sentent vulnérables à la cyberintimidation ressentent un besoin de formation. Pour eux, la formation initiale et continue est l'occasion de partager des expériences et d'analyser les méthodes de pratique professionnelle dans ce domaine. On croit encore que l'utilisation des outils numériques dans l'éducation est une façon d'enseigner ou un objet à enseigner aux élèves plutôt qu'une partie intégrante de leur culture générale. Une culture des sources et des pratiques d'information sur les risques numériques (recherche et veille) doit être développée. Il faut également renforcer la formation sur les enjeux du numérique et notamment sur les problèmes psycho-sociaux, éthiques, juridiques et techniques qui peuvent se poser dans l'utilisation des outils numériques et qui inquiètent les enseignants au point de les amener à renoncer à tout usage.

Ainsi, la connaissance des risques numériques peut influencer positivement les pratiques pédagogiques pour former les élèves à la culture numérique. Un enseignant ayant une forte culture numérique sera plus enclin à utiliser le numérique en classe avec ses élèves et à faire du numérique un objet d'enseignement-apprentissage.

L'influence évidente de la représentation des risques ne peut évoluer positivement sans une culture numérique générale et plurielle, complémentaire d'une culture de l'information au sens large, qui évite de diaboliser l'objet technique et permet d'en exploiter le potentiel pédagogique.

Il ne s'agit pas d'éduquer dans la peur, mais d'émanciper (et d'être émancipé, en tant qu'enseignant aussi) par une appréhension critique et éclairée du monde numérique.

***Retour au sommaire ☐***

## c) Boîte à outils de CYBER.EU.VET

Selon le plan d'éducation numérique 2021-2027, les compétences numériques et les défis de l'apprentissage sont également une priorité de l'agenda européen. La Commission européenne est déterminée à s'attaquer au déficit de compétences numériques et à promouvoir des projets et des

stratégies visant à améliorer le niveau des compétences numériques en Europe. Tous les Européens ont besoin de compétences numériques pour étudier, travailler, communiquer, accéder aux services publics en ligne et trouver des informations dignes de confiance. Cependant, de nombreux Européens ne disposent pas de compétences numériques adéquates. L'indice de l'économie et de la société numériques (DESI) montre que 4 adultes sur 10 et une personne sur trois qui travaille en Europe ne possèdent pas de compétences numériques de base. Les femmes sont également peu représentées dans les professions et les études liées à la technologie, puisque seulement un spécialiste des TIC sur six et un diplômé en sciences, technologie, ingénierie et mathématiques (STEM) sur trois sont des femmes.

La Commission européenne a fixé des objectifs dans le cadre de l'agenda européen des compétences et du plan d'action pour l'éducation numérique afin de garantir que 70 % des adultes disposent de compétences numériques de base d'ici 2025. Ces initiatives visent à réduire le niveau des jeunes de 13-14 ans ayant des résultats insuffisants en informatique et en culture numérique de 30% (2019) à 15% en 2030. La plateforme européenne sur les compétences et les emplois numériques est une nouvelle initiative lancée dans le cadre du programme "Connecting Europe Facility". Elle propose des informations et des ressources sur les compétences numériques, ainsi que des possibilités de formation et de financement[4].

### i. Cadres de compétence numérique du JRC/EC

- Cadre de compétence numérique pour les citoyens (DigComp)
- Cadre de compétence numérique pour les éducateurs (DigCompEdu)
- Cadre de compétence numérique pour les organisations éducatives (DigCompOrg) et outil d'autoréflexion pour les écoles (SELFIE)

*Pourquoi tous ces cadres ?*

- Renforcement des capacités pour la transformation numérique de l'E&T et pour relever les défis des compétences du 21e siècle.
- Cadres de référence fournissant une compréhension globale, complète et partagée : un langage commun.

*Quoi ?*

- Modèle conceptuel, niveaux de compétence et modules d'(auto-)évaluation.

4 Compétences et emplois numériques | Bâtir l'avenir numérique de l'Europe

- Les compétences sont définies comme des connaissances, des aptitudes et des attitudes.

### ii. Le DigComp 2.2

Plus de 250 nouveaux exemples de connaissances, de compétences et d'attitudes pour aider les prestataires d'éducation et de formation à mettre à jour leur programme et leur matériel de cours DigComp afin de relever les défis actuels.

La liste des compétences et des domaines de DigComp reste la même :

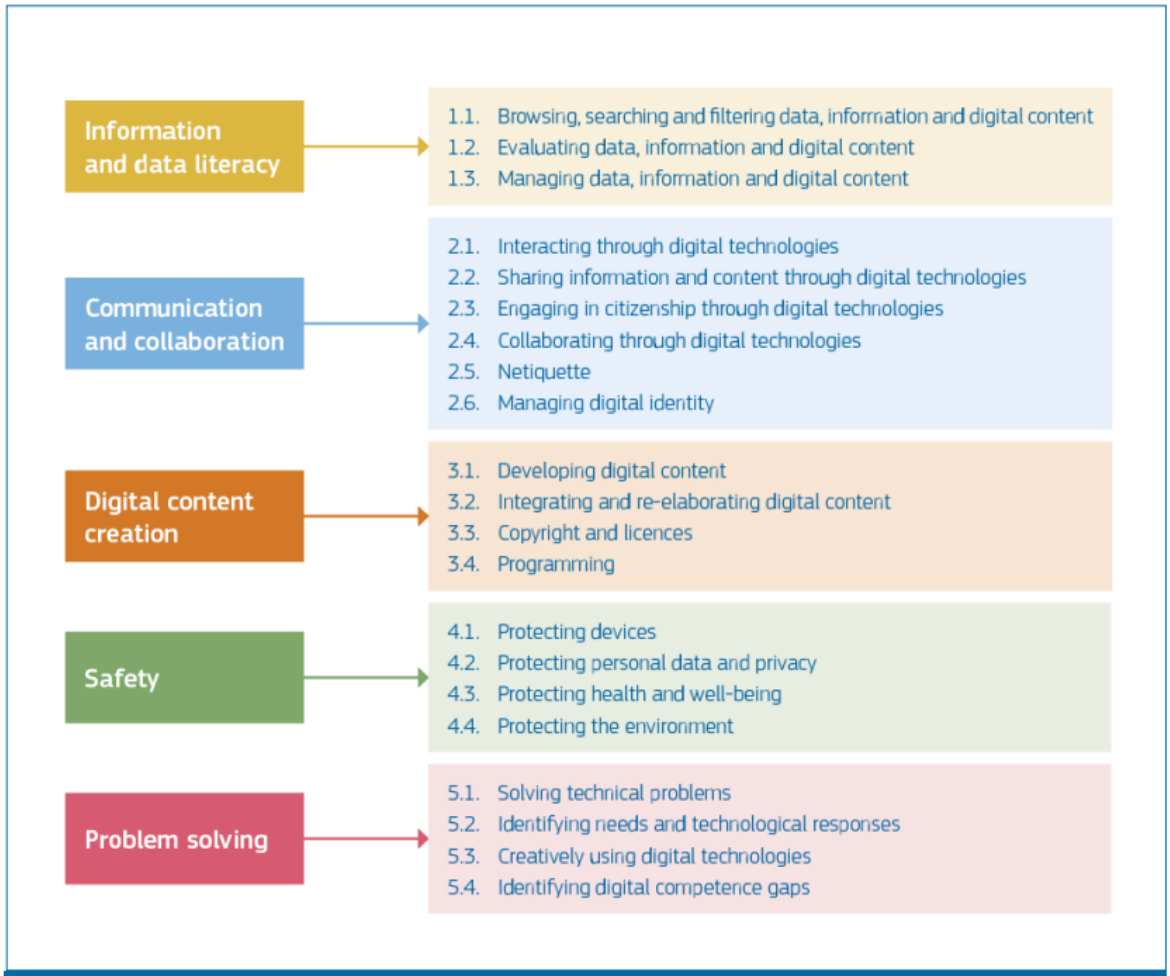



**FIG.1** The DigComp conceptual reference model [5]

L'un des thèmes clés de la mise à jour DigComp 2.2 est le bien-être et la sécurité. Dans chaque domaine, il y a 10 à 15 énoncés par compétence pour illustrer des thèmes contemporains d'actualité. Ils ne représentent pas une liste exhaustive de ce que la compétence elle-même implique et ils ne sont pas sur des niveaux de compétence, bien que certains soient plus complexes que d'autres, mais ils sont utiles pour la planification et la mise

[5] Commission européenne, Centre commun de recherche, Vuorikari, R., Kluzer, S., Punie, Y., DigComp 2.2, The Digital Competence framework for citizens : with new examples of knowledge, skills and attitudes, Office des publications de l'Union européenne, 2022,https://data.europa.eu/doi/10.2760/115376

à jour du curriculum et le développement du syllabus de formation DigComp ou du contenu des cours.

**SÉCURITÉ :** "protéger les appareils et le contenu numérique, et comprendre les risques et les menaces dans les environnements numériques. Connaître les mesures de sûreté et de sécurité et tenir compte de la fiabilité et de la vie privée."[6]

DIMENSION 1 • COMPETENCE AREA
4. SAFETY

DIMENSION 2 • COMPETENCE
4.1 PROTECTING DEVICES

To protect devices and digital content, and to understand risks and threats in digital environments.

To know about safety and security measures and to have a due regard to reliability and privacy.

DIMENSION 3 • PROFICIENCY LEVEL

| | | | |
|---|---|---|---|
| FOUNDATION | 1 | At basic level and with guidance, I can: | • **identify simple** ways to protect my devices and digital content, and<br>• differentiate simple risks and threats in digital environments.<br>• choose simple safety and security measures, and<br>• **identify simple** ways to have due regard to reliability and privacy. |
| | 2 | At basic level and with autonomy and appropriate guidance where needed, I can: | • **identify simple** ways to protect my devices and digital content, and<br>• differentiate simple risks and threats in digital environments.<br>• follow simple safety and security measures.<br>• **identify simple** ways to have due regard to reliability and privacy. |
| INTERMEDIATE | 3 | On my own and solving straightforward problems, I can: | • **indicate well-defined and routine** ways to protect my devices and digital content, and<br>• differentiate well-defined and routine risks and threats in digital environments, and<br>• **select well-defined and routine** safety and security measures.<br>• **indicate well-defined and routine** ways to have due regard to reliability and privacy |
| | 4 | Independently, according to my own needs, and solving well-defined and non-routine problems, I can: | • **organise** ways to protect my devices and digital content, and<br>• **differentiate** risks and threats in digital environments.<br>• **select** safety and security measures.<br>• **explain** ways to have due regard to reliability and privacy. |
| ADVANCED | 5 | As well as guiding others, I can: | • **apply different** ways to protect devices and digital content, and<br>• **differentiate a variety** of risks and threats in digital environments.<br>• **apply** safety and security measures.<br>• **employ different** ways to have due regard to reliability and privacy. |
| | 6 | At advanced level, according to my own needs and those of others, and in complex contexts, I can: | • **choose the most appropriate** protection for devices and digital content, and<br>• **discriminate** risks and threats in digital environments.<br>• **choose the most appropriate** safety and security measures.<br>• **assess the most appropriate** ways to have due regard to reliability and privacy. |
| HIGHLY SPECIALISED | 7 | At highly specialised level, I can: | • **create solutions to complex problems with limited definition** that are related to protecting devices and digital content, managing risks and threats, applying safety and security measures, and reliability and privacy in digital environments.<br>• **integrate my knowledge to contribute to professional practice and knowledge and guide others** in protecting devices. |
| | 8 | At the most advanced and specialised level, I can: | • **create solutions to solve complex problems with many interacting factors** that are related to protecting devices and digital content, managing risks and threats, applying safety and security measures, and reliability and privacy in digital environments.<br>• **propose new** ideas and processes to the field. |

7

### iii. Le DigCompEdu

[6] Luxembourg : Office des publications de l'Union européenne, 2018 KE-01-18-834-EN-N.pdf
[7] Ibidem

Le cadre européen pour la compétence numérique des éducateurs (DigCompEdu) est un cadre scientifique solide qui décrit ce que signifie la compétence numérique des éducateurs. Il fournit un cadre de référence général pour soutenir le développement de compétences numériques spécifiques aux éducateurs en Europe. DigCompEdu s'adresse aux éducateurs de tous les niveaux d'enseignement, de la petite enfance à l'enseignement supérieur et aux adultes, y compris l'enseignement et la formation généraux et professionnels, l'enseignement spécialisé et les contextes d'apprentissage non formels.
Le cadre DigCompEdu reflète les efforts menés au niveau international pour saisir et définir les compétences numériques spécifiques des enseignants et des formateurs.
L'objectif est de fournir un cadre à ceux qui travaillent dans le secteur de l'éducation et de l'enseignement supérieur et qui sont chargés de développer des modèles de compétences numériques, par exemple les décideurs politiques dans les États membres, les autorités régionales/locales, les organisations éducatives, les institutions (publiques ou privées) qui fournissent des services de formation et de développement professionnel.


Ainsi, la valeur ajoutée du cadre DigCompEdu est qu'il fournit :

- une base solide qui peut guider les politiques à tous les niveaux ;
- un modèle qui permet aux acteurs locaux de passer rapidement à l'élaboration d'un instrument concret, adapté à leurs besoins, sans avoir à développer une base conceptuelle pour ce travail ;
- un langage et une logique communs qui peuvent faciliter la discussion et l'échange des meilleures pratiques ;
- un point de référence permettant aux États membres et aux autres parties prenantes de valider l'exhaustivité et l'approche de leurs propres outils existants et futurs.

- l'approche de leurs propres outils et cadres existants et futurs.[8]

### iv. RENFORCER LES COMPÉTENCES NUMÉRIQUES DES EFP ÉDUCATEURS

L'utilisation ou le développement de cadres ou d'outils d'auto-évaluation est un bon moyen de déterminer le niveau de base des compétences numériques d'un éducateur. À partir de là, des activités de développement professionnel ciblées peuvent être mises en place. Le besoin croissant d'utiliser les technologies dans la pratique de l'enseignement s'accompagne de la nécessité de modifier la pédagogie afin de garantir que les outils numériques sont utilisés efficacement non seulement dans l'enseignement, mais aussi dans la conception et l'évaluation des cours. Le cadre européen des compétences numériques des éducateurs (DigCompEdu) décrit les principaux domaines de compétences requis par les éducateurs lorsqu'ils approfondissent leur engagement dans l'apprentissage et les pédagogies numériques. Les domaines de compétences clés sont présentés dans la figure ci-dessous (Redecker 2017).

[8] Redecker, C. European Framework for the Digital Competence of Educators: DigCompEdu. Punie, Y. (ed). EUR 28775 EN. Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-73494-6, doi:10.2760/159770, JRC107466

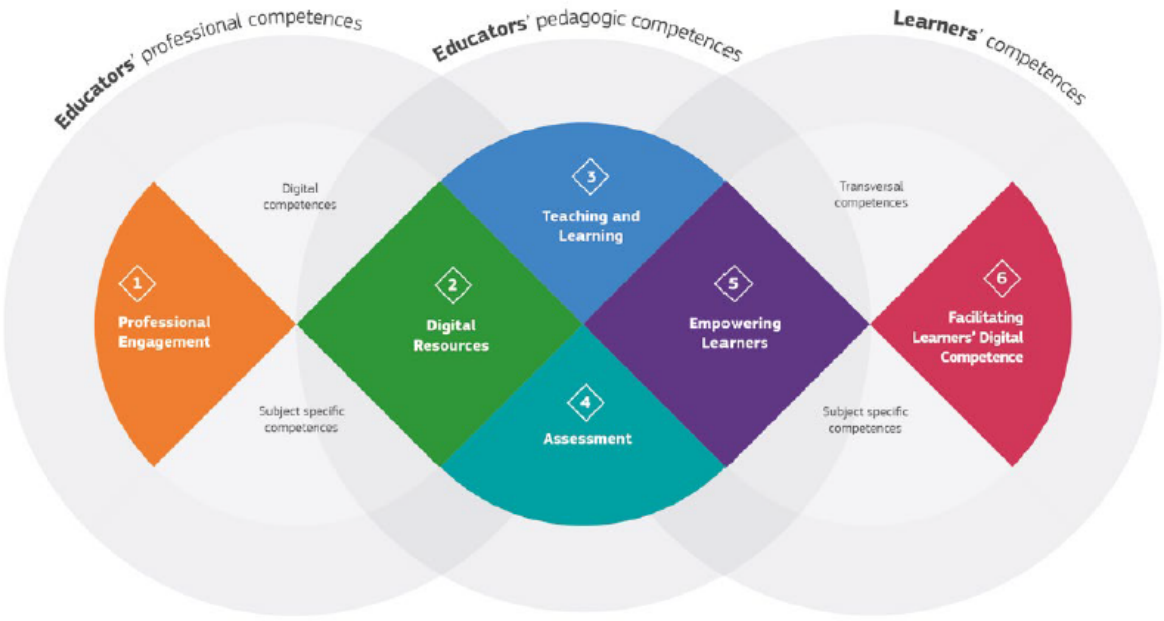


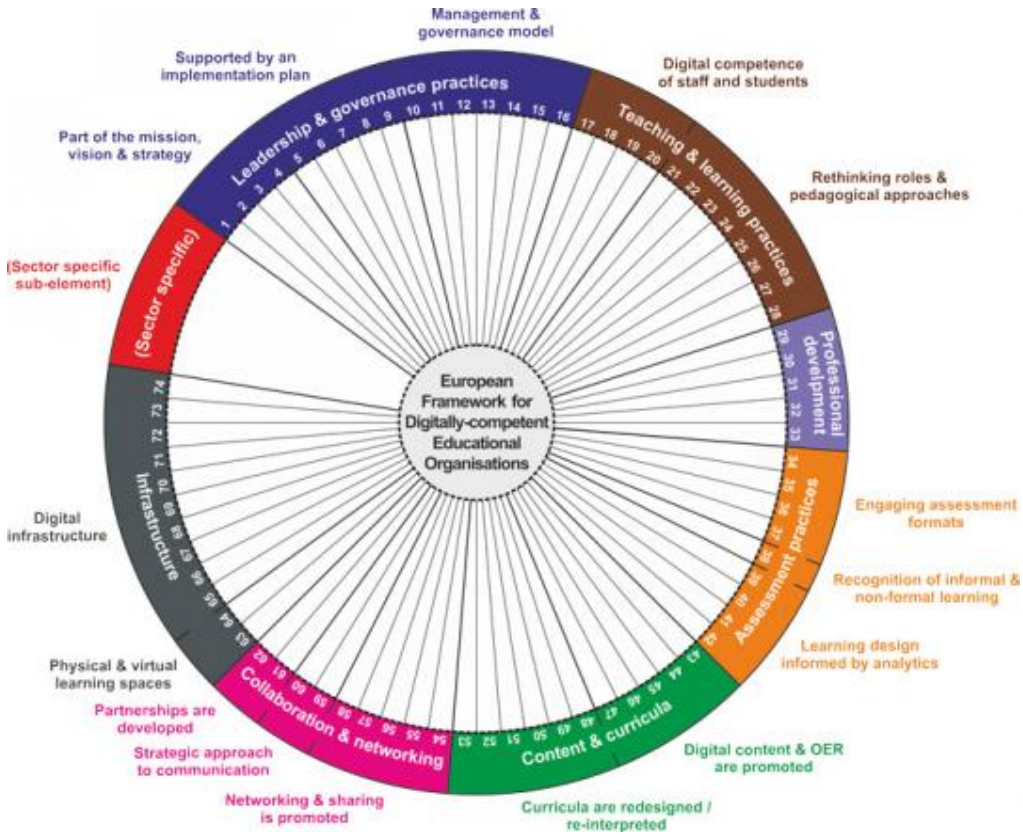

FIGURE 2: DIGCOMPEDU AREAS AND SCOPE

### v. Le cadre de référence DigCompOrg

Plusieurs cadres et outils d'auto-évaluation sont utilisés dans un certain nombre de pays européens, mais aucune tentative n'a été faite jusqu'à présent pour développer une approche paneuropéenne de la capacité numérique organisationnelle. Un cadre de référence européen qui adopte une approche systémique peut apporter une valeur ajoutée en favorisant la transparence, la comparabilité et l'apprentissage par les pairs. Le cadre DigCompOrg peut être utilisé par les organisations éducatives (c'est-à-dire les écoles primaires, secondaires et d'EFP, ainsi que les établissements d'enseignement supérieur) pour guider un processus d'autoréflexion sur leurs progrès vers une intégration complète et un déploiement efficace des technologies d'apprentissage numériques.

En outre, il peut faciliter la transparence et la comparabilité entre les initiatives connexes dans toute l'Europe, et il peut également jouer un rôle dans la lutte contre la fragmentation et le développement inégal dans les États membres. Le cadre DigCompOrg peut également être utilisé comme un outil de planification stratégique pour les décideurs politiques afin de promouvoir des politiques globales pour l'adoption efficace des technologies d'apprentissage numériques par les organisations éducatives au niveau régional, national et européen. Il peut

également être utilisé comme un moyen de sensibiliser à l'approche systémique nécessaire à l'utilisation efficace des technologies numériques d'apprentissage.




es principaux objectifs de DigCompOrg sont :

- d'encourager l'autoréflexion et l'auto-évaluation au sein des organisations éducatives au fur et à mesure qu'elles approfondissent leur engagement dans l'apprentissage et les pédagogies numériques ;
- permettre aux décideurs politiques (au niveau local, régional, national et international) de concevoir, mettre en œuvre et évaluer des programmes, des projets et des interventions politiques pour l'intégration des technologies d'apprentissage numérique dans les systèmes d'éducation et de formation.

### vi. SELFIE

SELFIE pour l'apprentissage par le travail (WBL) est un outil en ligne gratuit qui aide les écoles et les entreprises d'enseignement et de formation professionnels (EFP) à tirer le meilleur parti des technologies numériques pour l'enseignement, l'apprentissage et la formation. SELFIE WBL aide les écoles et les entreprises à s'adapter à l'ère numérique. De cette façon, il soutient la transition numérique, l'une des principales priorités politiques de la Commission européenne. L'adaptation de SELFIE aux exigences spécifiques du WBL est une étape nécessaire **pour soutenir les écoles d'EFP**.[9]

Au total, 35 000 participants issus d'environ 150 écoles d'EFP et 250 entreprises en France, en Allemagne, en Hongrie, en Pologne, en Roumanie, en Géorgie, au Monténégro et en Turquie ont été impliqués dans le pilotage. Les résultats de ces pilotes peuvent être téléchargés [LIEN vers les ressources][10].

Le Forum européen de l'enseignement et de la formation techniques et professionnels (EfEFP) et la Fondation européenne pour la formation (FEF) ont apporté un soutien inestimable tout au long du projet.

***Retour au sommaire ☐***

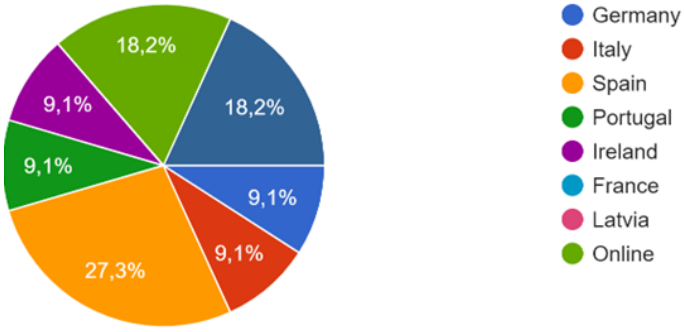
## d)Directives CYBER.EU.VET

Le projet CYBER.EU.VET visait à renforcer la capacité de l'enseignement et de la formation professionnels européens à reconnaître et à gérer les menaces de cybersécurité (par

[9] SELFIE pour l'apprentissage par le travail | European Education Area (europa.eu)
[10] Ressources SELFIE | European Education Area (europa.eu)

exemple, les attaques de phishing, les botnets, les fraudes financières et bancaires, les fraudes de données) dans un contexte historique où la formation en ligne est de plus en plus utilisée.
Pour ce faire, il a amélioré les aptitudes et les compétences des éducateurs de l'EFP en matière de gestion des menaces de cybersécurité, compte tenu de leur rôle central dans le transfert de connaissances des bonnes pratiques et des compétences à leurs étudiants, et a également sensibilisé les enseignants de l'EFP, les étudiants et leurs familles à l'importance de reconnaître ces risques quotidiens, qui peuvent avoir un impact économique et social sur tous les citoyens européens. Le projet s'est appuyé sur une circulation conjointe locale, nationale et transnationale des capacités et de l'expertise et sur un bon niveau d'accès et d'utilisation de l'information numérique.

**8 Sessions de Gamejam avec 54 étudiants et 15 formations nationales spécifiques pour les formateurs** ont été organisées pour débattre des résultats de la recherche, des outils numériques partagés et des nouveaux outils créés, en échangeant des expériences et des considérations pour développer une sorte de "récit collectif thématique" préparatoire au passage de l'exploration et de l'analyse à la gestion et à la résolution de problèmes numériques.




Ces événements ont permis aux jeunes de travailler ensemble et de montrer que même les institutions perçues comme éloignées du citoyen moyen (par exemple la Commission européenne) offrent des opportunités intéressantes pour la population jeune.

Dans ce guide, une **session de formation** est définie comme une session de formation unique qui se déroule au cours d'une journée ou d'une partie de la journée. Elle peut durer 30 minutes, une heure ou même une journée entière. Une session de formation peut comporter des pauses tout au long de la journée et couvrir un ou plusieurs sujets. Une session peut se dérouler dans une salle de classe, dans un petit groupe avec une seule famille, ou même en tête-à-tête. Aux fins du présent guide, un programme de formation est

un ensemble de sessions de formation qui complètent un cycle de formation. Par exemple, une agence peut proposer un programme de formation de 8 semaines, une fois par semaine. Le programme de formation pourrait ensuite être relancé pour un nouveau groupe de personnes. (Ateliers et cours, 2021)

## I. La base d'un atelier : Connaissances, compétences et attitudes

Ce guide suit un cadre de sensibilisation des apprenants aux menaces numériques, qui repose sur les connaissances, les aptitudes et les compétences. De même, les superviseurs de programmes et les enseignants/formateurs améliorent leurs connaissances, leurs aptitudes et leurs attitudes afin d'être plus efficaces. Cette section se penche sur les connaissances, les aptitudes et les attitudes des enseignants et des formateurs.

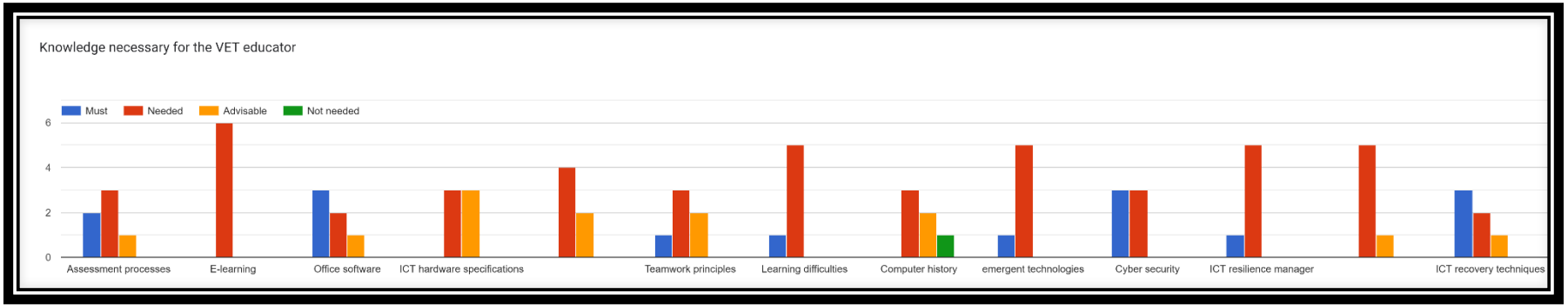
**Les connaissances, les compétences et les attitudes sont les fondements d'une formation efficace**. Les formateurs efficaces ont des connaissances, des compétences et des attitudes concernant la formation et les sujets qu'ils enseignent, et les programmes et sessions de formation qu'ils dispensent doivent inclure des connaissances, des compétences et des attitudes pour les participants qui sont concentrés sur le sujet et le contenu.

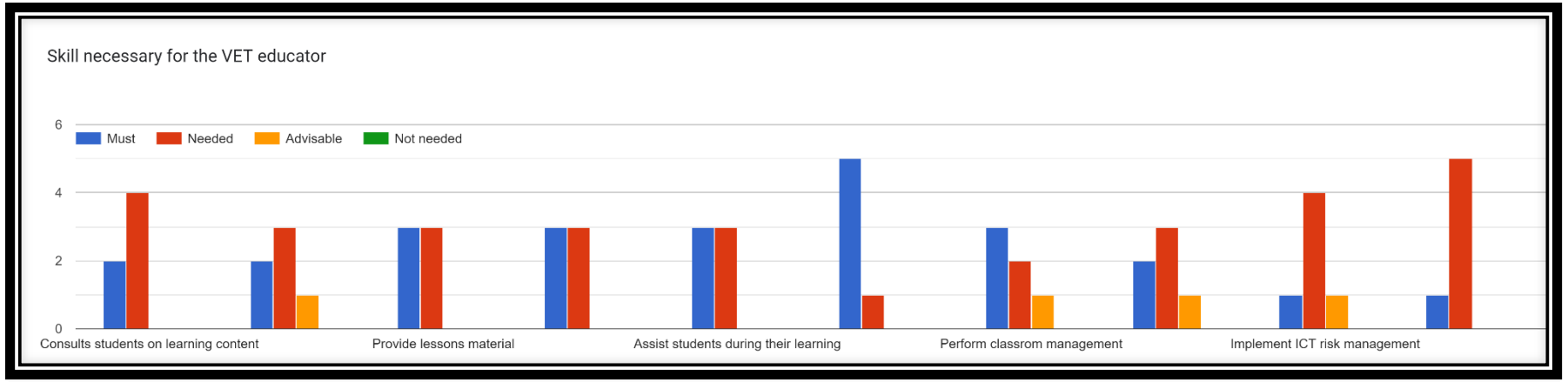
**Question à soi-même : À qui pouvez-vous vous adresser si vous avez des questions sur les normes et le contenu du programme en tant que nouveau praticien de l'EFP ?**

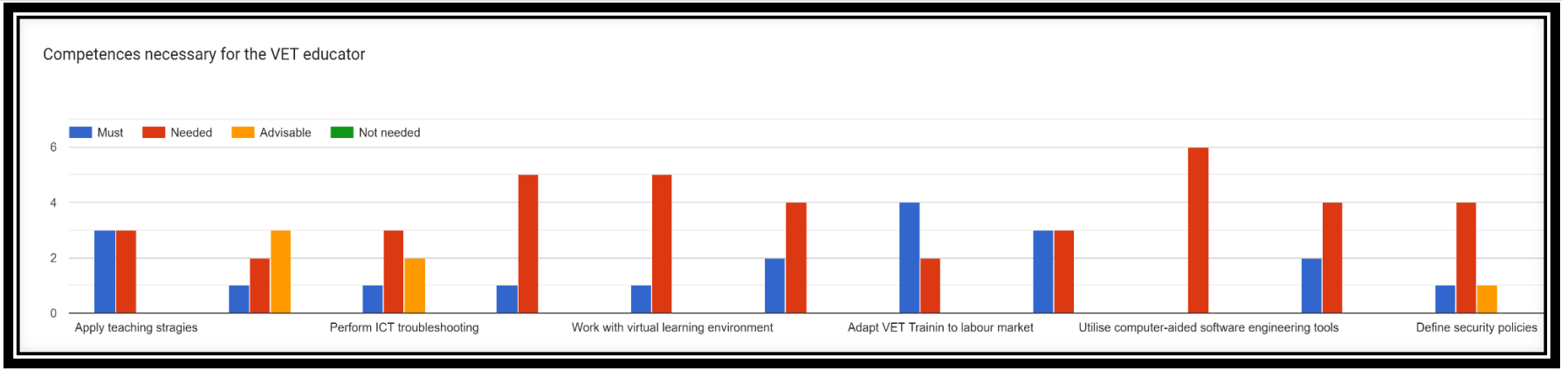
Les formateurs doivent avoir une large compréhension du contenu de base afin de pouvoir répondre aux questions qui peuvent se poser. Si un praticien ne connaît pas la réponse à une question, il est essentiel qu'il déclare qu'il ne connaît pas la réponse mais qu'il l'étudiera et en rendra compte. Les praticiens ne doivent pas donner de fausses informations ou inventer des réponses dans l'intérêt du bien-être et de la compréhension des participants. Il incombe au formateur de faire des recherches, de trouver des réponses et de faire un suivi auprès des participants pour s'assurer qu'ils reçoivent des informations exactes.

**Voulez-vous en savoir plus sur ce qu'un enseignant peut faire lorsqu'il traite de ce sujet ?**

Voici des exemples de connaissances, de compétences et d'attitudes appropriées qu'un formateur efficace devrait posséder selon les partenaires du consortium.




Co-funded by the
Erasmus+ Programme
of the European Union

**Activité: En tant qu'enseignant/formateur, quels sont quelques exemples de vos connaissances, compétences et attitudes ? Remplissez les cases vides du tableau. Un exemple est donné.**

| Exemples de connaissances | Exemples de compétences | Exemples d'attitudes |
|---|---|---|
| Je suis familier avec la cybersécurité et les technologies émergentes. | Je peux développer des supports pédagogiques numériques et adapter l'enseignement au groupe cible. | J'ai à cœur de rendre les sessions aussi efficaces que possible pour nos participants, et je m'engage à le faire. |
| | | |
| | | |
| | | |
| | | |
| | | |

- **Connaissance** : Résultat de l'assimilation d'informations par l'apprentissage. La connaissance est l'ensemble des faits, principes, théories et pratiques liés à un domaine d'étude ou de travail.
- **Compétence** : Capacité à appliquer des connaissances et à utiliser un savoir-faire pour accomplir des tâches et résoudre des problèmes.
- **Compétence**: Capacité à appliquer les résultats d'apprentissage de manière adéquate dans un contexte défini (éducation, travail, développement personnel ou professionnel. [11]

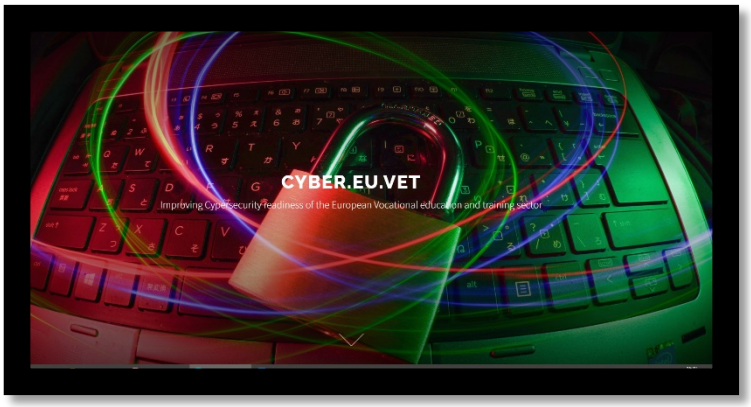
*Retour au sommaire* ↑

## II. Le site CYBER.EU.VET

[11] Le cadre européen des certifications pour l'éducation et la formation tout au long de la vie (CEC)

Co-funded by the Erasmus+ Programme of the European Union

Le consortium du projet a créé dès la première étape du projet un site web dédié développé avec des technologies open-source (Wordpress) et une approche modulaire, qui peut permettre à de nouveaux partenaires de différents pays d'ajouter et de gérer leurs propres contenus (une fois qu'ils ont accepté les termes et conditions établis par les partenaires du projet). Les plateformes numériques comme CYBER.EU.VET one peuvent être ouvertes de deux manières pour promouvoir l'innovation et la génération de valeur (Boudreau 2010) .




Bien sûr, les plateformes numériques, et dans ce cas précis la plateforme conçue comme ressource éducative ouverte, peuvent être exploitées davantage pour les activités de suivi. Ce nouveau système permet de mettre en relation le monde physique traditionnel avec une interface numérique capable de connecter et d'organiser la demande et l'offre d'un outil ou d'un service dans un espace virtuel unique.

**Karhu, Gustafsson, and Lyytinen:** *Exploiting and Defending Open Digital Platforms*
Information Systems Research, 2018, vol. 29, no. 2, pp. 479–497, © 2018 The Author(s)

Table 1. Two Forms of Platform Openness and Related Resources

| Platform openness | Boundary resources | Shared resources | Actor who shares | Type of sharing | Platform owner's rationale |
|---|---|---|---|---|---|
| Access openness | API, app store | Complement, e.g., apps | Complementor | Shared for distribution | Generate network effects, and extract value from complementarities |
| Resource openness | Open-source license | Platform core, e.g., AOSP | Platform owner | Shared IPR | Strategic forfeiture of IPR while recovering costs from somewhere else |

Ces plateformes créent des réseaux qui relient les personnes et les services dans le temps.

**L'intégrité du réseau est liée non seulement aux facteurs de l'infrastructure d'information, à sa sécurité et au flux de données au sein du réseau, mais aussi aux changements sociaux et environnementaux qui interfèrent avec les composantes humaines.**

C'est pour cette raison qu'on a organisé une campagne à effet multiplicateur pour diffuser et faire connaître les outils technologiques et le manuel CYBER.EUY.VET développés.

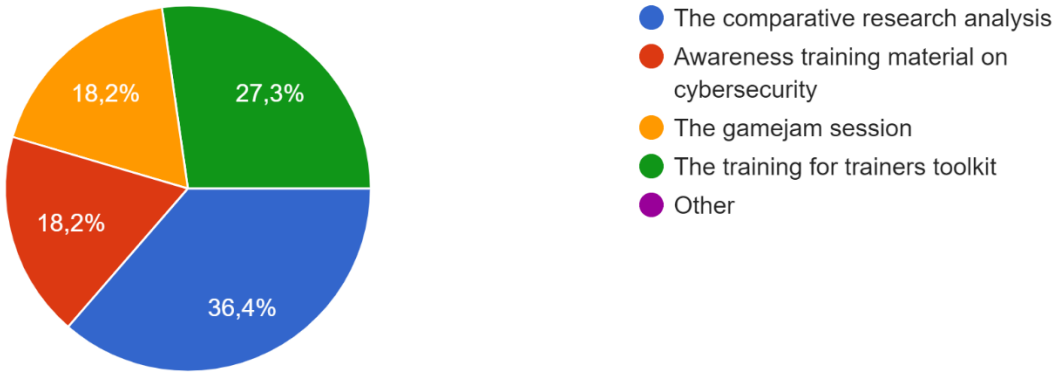
Cette campagne avait également pour objectif de sensibiliser les enseignants de l'EFP, les étudiants et leurs familles à l'importance de reconnaître ces risques quotidiens, qui peuvent avoir un impact économique et social sur tous les citoyens européens..

Les systèmes TIC tirent parti de l'"effet réseau" émergent en combinant les médias sociaux ouverts en ligne, la création de connaissances distribuées et les données provenant d'environnements réels afin **de sensibiliser aux problèmes et aux solutions possibles en demandant des efforts collectifs, ce qui permet de nouvelles formes d'innovation sociale.**

## *III. "Une perspicacité de praticien"*

Les partenaires et les praticiens ayant été impliqués dans le projet CYBER.EU.VET ont affirmé avoir bénéficié de leurs objectifs de recherche grâce à une meilleure compréhension de la perception des étudiants en cybersécurité dans le contexte local et européen. Les échanges entre des parties prenantes si différentes les unes des autres ont été l'occasion d'acquérir des perspectives et des approches différentes sur des questions communes et d'apprendre à les traduire dans un langage plus commun. Selon les mots de notre partenaire : "Il a été très bénéfique d'en apprendre davantage sur l'état actuel des connaissances dans le domaine de la cybersécurité et sur les principales cybermenaces dans les pays partenaires. Il est également intéressant de connaître et de pouvoir suivre les tendances en termes de cyberattaques qui semblent être très similaires dans chaque pays". 81,8% des partenaires ont déclaré qu'ils avaient l'intention d'utiliser le matériel partagé ou créé dans le cadre du projet CYBER.VET.EU à l'avenir, 36,4% au niveau local, 36,4% au niveau national et 27,3% au niveau international, à travers des sessions de formation et des ateliers, des forums et bien sûr, les médias sociaux.
Le contexte des pays participant au projet est très différent les uns des autres, bien qu'en tant que pays européens ils partagent certaines similitudes. La cybersécurité est très évolutive, car les menaces changent au fil du temps. Il est donc intéressant que les résultats obtenus soient mis à jour par les formateurs et les chercheurs afin qu'ils soient valables au moment où ils sont utilisés.

Le graphique qui montre quels outils partagés ont été les plus utiles pour les opérateurs des différents services des 8 partenaires du consortium est significatif :




## IV. Une note finale

Le manuel CYBER.EU.VET a été conçu pour aider les formateurs de l'EFP et les praticiens du numérique à utiliser les outils de cybersécurité ainsi que les instructions sur la manière d'utiliser le matériel CYBER.EU.VET listé en annexe. Il fournit des suggestions sur la façon dont la formation peut être organisée, ainsi que des recommandations opérationnelles pour permettre aux praticiens de fournir aux étudiants les connaissances et les outils dont ils ont besoin pour reconnaître les menaces de cybersécurité. Cet e-book a été conçu à l'intention des enseignants de l'EFP, des étudiants de l'EFP, des familles des étudiants et des institutions de l'EFP au niveau international ou local. Les praticiens (ou les travailleurs sociaux/gestionnaires de cas) qui dispensent la formation et l'orientation, les superviseurs ou les coordinateurs de la formation, et ceux qui dispensent l'orientation, tels que les bénévoles, les stagiaires, les autres membres du personnel d'aide à la réinstallation, les autres prestataires de services et les membres de la communauté, peuvent tous en bénéficier. Une sensibilisation accrue aux risques liés aux fraudes de données, aux logiciels malveillants et aux autres menaces à la sécurité en ligne, à tous les niveaux, de la direction de l'établissement d'EFP aux familles des étudiants, est une étape fondamentale pour protéger les citoyens de l'UE des dommages causés par les menaces à la cybersécurité, à un moment déjà caractérisé par une crise historique.

Cet e-book contient plusieurs suggestions qui, nous l'espérons, inciteront les enseignants et les praticiens de l'EFP à repenser les objectifs de leur formation et la manière dont ils pourraient améliorer la qualité de l'enseignement, en développant des méthodes innovantes d'apprentissage en ligne.

# e) Annexe

I. Glossaire

II. Le guide de l'utilisateur de CYBER.EU.VET - guide d'orientation pour les futures implémentations

# I. GLOSSAIRE

**DONNÉES**
séquence d'un ou plusieurs symboles à laquelle on donne un sens par un ou plusieurs actes d'interprétation spécifiques (les données n'ont pas de sens intrinsèque). Les données peuvent être analysées ou utilisées dans le but d'acquérir des connaissances ou de prendre des décisions. Les données numériques sont représentées à l'aide du système numérique binaire composé de uns (1) et de zéros (0), par opposition à leur représentation analogique.[12]

**COMMUNICATION NUMÉRIQUE**
Communication utilisant la technologie numérique. Il existe différents modes de communication, par exemple la communication synchrone (communication en temps réel, par exemple en utilisant Skype, le chat vidéo ou Bluetooth) et la communication asynchrone (communication non simultanée, par exemple le courrier électronique, les SMS) en utilisant par exemple les modes un à un, un à plusieurs ou plusieurs à plusieurs.[13]

**COMPÉTENCE NUMÉRIQUE**
La compétence numérique peut être définie de manière générale comme l'utilisation confiante, critique et créative des TIC pour atteindre des objectifs liés au travail, à l'employabilité, à l'apprentissage, aux loisirs, à l'inclusion et/ou à la participation à la société.[14]

**CONTENU NUMÉRIQUE**
Tout type de contenu qui existe sous la forme de données numériques codées dans un format lisible par une machine, et qui peut être créé, visualisé, distribué, modifié et stocké à l'aide de technologies numériques. Parmi les exemples de contenu numérique, citons : les pages web et les sites web, les médias sociaux, les données et les bases de données, les fichiers audio numériques, tels que les mp3, et les livres électroniques, l'imagerie numérique, la vidéo numérique, les jeux vidéo, les programmes informatiques et les logiciels. Dans le cadre de DigCompEdu, le contenu numérique est divisé en ressources et données numériques.[15]

**ENVIRONNEMENT NUMÉRIQUE**
un contexte, ou un "lieu", qui est rendu possible par la technologie et les dispositifs numériques, souvent transmis par l'internet ou d'autres moyens numériques, par exemple le réseau de téléphonie mobile. Les enregistrements et les preuves de l'interaction d'un individu avec un environnement numérique constituent son empreinte numérique. Dans DigComp, le terme d'environnement numérique est utilisé comme toile de fond pour les actions numériques sans nommer une technologie ou un outil spécifique.

[12] Modifié de: fr.wikipedia.org/wiki/Donn%C3%A9e_(informatique)
[13] Source: *DigComp Framework* https://ec.europa.eu/jrc/digcomp
[14] *Ibidem*
[15] Redecker, C. European Framework for the Digital Competence of Educators: DigCompEdu. Punie, Y. (ed). EUR 28775 EN. Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-73494-6, doi:10.2760/159770, JRC107466

## SERVICE NUMÉRIQUE

permet à un utilisateur (citoyen, consommateur) de créer, traiter, stocker ou accéder à des données sous forme numérique et de partager ou d'interagir avec des données sous forme numérique téléchargées ou créées par le même utilisateur ou d'autres utilisateurs de ce service (directive (UE) 2019/770).

## TECHNOLOGIE NUMÉRIQUE

Tout produit pouvant être utilisé pour créer, visualiser, distribuer, modifier, stocker, récupérer, transmettre et recevoir des informations sous forme numérique par voie électronique. Par exemple, les ordinateurs et les appareils personnels (par exemple, un ordinateur de bureau, un ordinateur portable, un netbook, un ordinateur tablette, des téléphones intelligents, des PDA avec des fonctions de téléphonie mobile, des consoles de jeux, des lecteurs de médias, des lecteurs de livres électroniques), la télévision numérique, les robots.[16]

## OUTILS NUMÉRIQUES

Technologies numériques utilisées dans un but donné ou pour remplir une fonction particulière, par exemple le traitement de l'information, la communication, la création de contenu, la sécurité ou la résolution de problèmes.[17]

## CONTENU ÉDUCATIF

Contenu (numérique) pertinent, d'une manière ou d'une autre, pour le contexte éducatif. Ce terme est plus large que celui de "ressource éducative" dans la mesure où il comprend également le contenu marginal au processus d'enseignement, par exemple la communication avec les étudiants, les parents, les collègues ; le contenu administratif, etc.[18]

## RESSOURCES ÉDUCATIVES

Ressources (numériques ou non) conçues et destinées à être utilisées à des fins éducatives.[19]

## LITTÉRATIE MÉDIATIQUE

Désigne les compétences, les connaissances et la compréhension qui permettent aux citoyens d'utiliser les médias de manière efficace et sûre. Afin de permettre aux citoyens d'accéder à l'information et d'utiliser, d'évaluer de manière critique et de créer des contenus médiatiques de manière responsable et sûre, les citoyens doivent posséder des compétences avancées en matière d'éducation aux médias. L'éducation aux médias ne doit pas se limiter à l'apprentissage des outils et des technologies, mais doit viser à doter les citoyens de l'esprit critique nécessaire pour exercer leur jugement, analyser des réalités complexes et reconnaître la différence entre une opinion et un fait. [20]

## RESSOURCES ÉDUCATIVES OUVERTES

Matériel d'enseignement, d'apprentissage et de recherche sur tout support, numérique ou autre, qui est dans le domaine public ou qui a été publié sous une licence ouverte permettant l'accès gratuit, l'utilisation, l'adaptation et la redistribution par d'autres sans restriction ou avec des restrictions limitées.[21]

## AUTO-ÉVALUATION

L'auto-évaluation implique la capacité de juger de manière réaliste ses propres performances. Les partisans de l'auto-évaluation suggèrent qu'elle présente de nombreux avantages, par exemple : elle fournit un retour d'information opportun et

[16] Modifié à partir de la source: http://www.tutor2u.net/business/ict/intro_what_is_ict.htm
[17] *Ibidem*
[18] *Ibidem*
[19] *Ibidem*
[20] Source: the EU's Audiovisual Media Services Directive (2018)
[21] Source: UNESCO definition http://www.unesco.org/new/en/communication-and-information/access-to-knowledge/open-educational-resources/what-are-open-educational-resources-oers/

efficace et permet aux étudiants d'évaluer rapidement leur propre apprentissage ; elle permet aux instructeurs de comprendre et de fournir un retour d'information rapide sur l'apprentissage ; elle favorise l'intégrité académique grâce à l'auto-évaluation par l'étudiant de ses progrès d'apprentissage ; favorise les compétences de pratique réflexive et d'auto-contrôle ; développe l'apprentissage autorégulé ; augmente la motivation de l'étudiant ; améliore la satisfaction de participer à un environnement d'apprentissage collaboratif ; aide les étudiants à développer une série de compétences personnelles et transférables pour répondre aux attentes des futurs employeurs.[22]

**INCLUSION SOCIALE**

Processus visant à améliorer les conditions de participation des individus et des groupes à la société (par la Banque mondiale). L'inclusion sociale vise à donner aux personnes pauvres et marginalisées les moyens de tirer parti des opportunités mondiales en plein essor. Elle garantit que les personnes ont leur mot à dire dans les décisions qui affectent leur vie et qu'elles bénéficient d'un accès égal aux marchés, aux services et aux espaces politiques, sociaux et physiques.[23]

**ENVIRONNEMENT STRUCTURÉ**

où les données résident dans un champ fixe au sein d'un enregistrement ou d'un fichier, par exemple les bases de données relationnelles et les feuilles de calcul. La réponse/solution technologique fait référence à la tentative d'utiliser la technologie (et/ou l'ingénierie) pour résoudre un problème.

[22] Source: *Cornell University Centre for Teaching Excellence* http://www.cte.cornell.edu/

[23] Source: *DigComp Framework* https://ec.europa.eu/jrc/digcomp

# Bibliographie

Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

Ala-Mutka, K. (2011). Mapping Digital Competence: Towards a Conceptual Understanding. (JRC Technical Notes No. JRC67075). IPTS.

Baron G.-L. et Baudé J. (1992), L'intégration de l'informatique dans l'enseignement et la formation des enseignants, Tours: EPI - INRP.

BIBB (2016), "Economy 4.0 needs Education 4.0", Strengthening the media competence of training staff and trainees.

https://doi.org/10.13140/RG.2.2.18046.00322
Brodnik, A., Csizmadia, A., Futschek, G., Kralj, L., Lonati, V., Micheuz, P., & Monga, M. (2021). Programming for All: Understanding the Nature of Programs. ArXiv:2111.04887 [Cs].

http://arxiv.org/abs/2111.04887
Buisán García,M.; Valdés, F. (2017), La industria Conectada 4.0., Revista de economía, No 898.

Bihouix P, Mauvilly, K (2016), Le Désastre de l'école numérique, Le Seuil.

Carretero, S., Vuorikari, R., & Punie, Y. (2017). DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use. Publica-tions Office of the European Union.
https://data.europa.eu/doi/10.2760/38842

Cyber Ireland, (2021), Cyber Security Skills Report 2021: National Survey: https://www.cyberireland.ie/wp-content/uploads/2021/02/Cyber-Ireland-Skills-Report2021.pdf (accessed on 3rd July, 2021).

EFVET (2021), Digital Balance: Balancing Digital Competences and Wellbeing.

European Commission. (2022). Translations of DigComp 2.0 in the European Skills, Competences and Occupa-tions classification (ESCO). Publications Office of the Eu-ropean Union. DOI:10.2767/316971

European Union. (2018). Council Recommenda-tion of 22 May 2018 on key competences for lifelong learning (ST/9009/2018/INIT).

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:O-J.C_.2018.189.01.0001.01.ENG
Ferrari, A. (2012). Digital competence in practce: An anal-ysis of frameworks. Publications Office of the European Union.

https://data.europa.eu/doi/10.2791/82116
Ferrari, A. (2013). DIGCOMP: A framework for developing and understanding digital competence in Europe. Publi-cations Office. doi:10.2788/52966

Ferrari, A., Brecko, B., & Punie, Y. (2014). DIGCOMP: a Framework for Developing and Understanding DigitalCompetence in Europe. ELearning Papers, 38, 1–14.

Ferrari, A., Punie, Y., & Redecker, C. (2012). Understand-ing digital competence in the 21st century: An analysis of current frameworks. In EC-TEL 2012: 21st Century Learning for 21st Century Skills (pp. 79–92).

Government of Latvia, (2020), Digital Transformation Guidelines 2021-2027.

Huismann, A. (2020), Vocational education and training for the future of work: Germany, Cedefop ReferNet thematic perspectives series.

Information Technology Security Incident Response Institution, (2021), CERT.LV Annual Report 2020.

Izglītības un zinātnes ministrija (2017), Informatīvais ziņojums "Priekšlikumi konceptuāli jaunas kompetencēs balstītas izglītības prasībām atbilstošas skolotāju izglītības nodrošināšanai Latvijā.

Izglītības un zinātnes ministrija (2020), Pedagogiem nodrošināta iespēja bez maksas pilnveidot digitālās prasmes.

Janssen, J., & Stoyanov, S. (2012). Online Consultation on Experts' Views on Digital Competence. Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC73694

Kampylis, P, Punie, Y & Devine, J 2015, Promoting effective digital-age learning: a European framework for digitally competent educational organisations, Publications Office of the European Union, Luxembourg

Microsoft Digital Defense Report. https://www.microsoft.com/de/security/business/security-intelligence-report

Ministry of Education, University and Research, Government of Italy (2021), Innovare e potenziare le competenze digitali nella scuola, Memorandum of Understanding n. 785 of 22 January 2021

Ministry of Technological Innovation and Digital Transition (2020), 2025 – Strategia per l'innovazione tecnologica e la digitalizzazione del Paese.

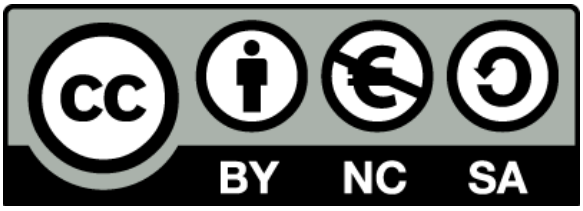
OECD. (2014). Assessing problem-solving skills in PISA 2012. In PISA 2012 Results: Creative Problem Solv-ing (Volume V): Students' Skills in Tackling Real-Life Problems. OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264208070-6-en

Vuorikari, R., Punie, Y., Carretero Gomez, S., & Van den Brande, L. (2016). DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptu-al Reference Model. Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC101254

# DISCLAIMER

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Il est possible de retrouver le document grâce au code QR suivant :




***Retour au sommaire ☐***