YBER.EU.VET

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

CYBER.EU.VET

KA226 - Partenariats pour la préparation à l'éducation numérique

Project N. 2020-1-DE02-KA226-C31C2976

Rapport du Consortium

sur les principaux défis et les meilleures pratiques en matière de cybersécurité

YBER.EU.VET

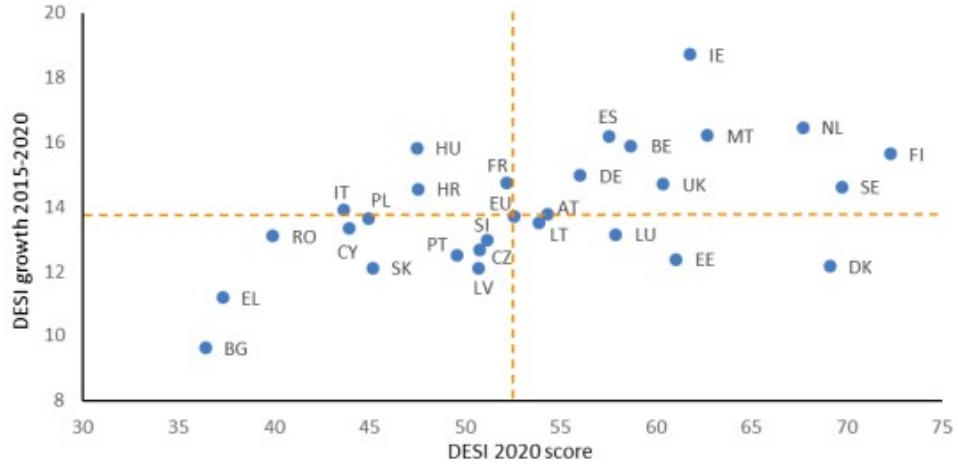
Co-funded by the
Erasmus+ Programme
of the European Union

Table des matières

Introduction

Le monde étant de plus en plus numérisé, il est devenu plus évident que la pratique doit être combinée avec la politique actuelle. L'accent est mis sur les politiques de culture numérique et de cybersécurité dans le contexte européen, mais il existe moins d'exemples d'initiatives qui sont considérées comme remplissant ces objectifs en accord avec les politiques développées. Pour observer attentivement dans quelle mesure les compétences numériques et la cybersécurité constituent un sujet central et divergent, il est utile de considérer l'indice 2020 de l'économie et de la société numériques (DESI).

Dans le cadre de son tableau général, le DESI surveille les performances numériques globales de l'Europe et mesure le niveau de compétitivité numérique des pays de l'UE. En fournissant des informations sur l'état de la numérisation dans chaque État membre, il permet d'identifier les domaines dans lesquels il convient d'investir et de prendre des mesures supplémentaires. Pour un avenir numérique adapté aux besoins des personnes et respectueux des valeurs fondamentales de l'UE, la Commission a présenté une vision de la transformation numérique "Shaping Europe's digital future" en février 2020. Le rapport DESI 2020 évalue l'économie et la société numériques au début de la pandémie en utilisant les données de 2019.



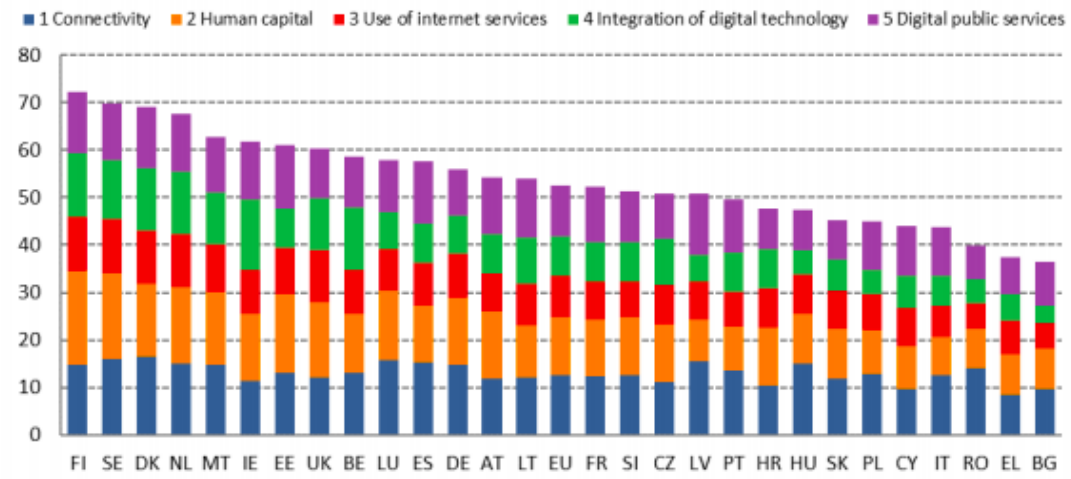
Source: DESI 2020, European Commission.

Plus précisément, cet indice étudie et rassemble des données sur :

- Connectivité : La disponibilité d'un accès rapide et fiable à l'internet (y compris les connexions fixes et mobiles) est essentielle à l'ère actuelle de la fourniture en ligne de services sociétaux et économiques clés ;
- le capital humain : L'épine dorsale de la société numérique est constituée par les compétences numériques de ses habitants. Les utilisateurs de services numériques et les personnes dont la mobilité est limitée peuvent s'engager dans des activités de base en ligne grâce à ces dispositifs ;
- Utilisation de l'internet : Au fur et à mesure de la progression de la pandémie, de plus en plus de personnes ont utilisé Internet. Le confinement généralisé a entraîné un accès régulier aux médias sociaux et aux plateformes de divertissement, ainsi qu'aux services de télétravail et de commerce électronique ;
- Intégration de la technologie numérique : Les entreprises ont rapidement adopté de nouvelles modalités de travail pour s'adapter aux mesures gouvernementales qui réduisaient les interactions sociales ;

- Au milieu des mesures de distanciation sociale, il est nécessaire de poursuivre les activités gouvernementales pour s'assurer que les services publics numériques apportent des avantages. Il faudra des services publics numériques solides dans tous les États membres pour réussir la stratégie de sortie de la pandémie actuelle.

Une telle analyse est utile lorsque l'on considère le consortium de partenaires dont les pays membres se différencient fortement en termes de performances numériques et de cybersécurité. En effet, trois d'entre eux (dans l'ordre, l'Irlande, l'Espagne et l'Allemagne) obtiennent un meilleur score que la moyenne de l'UE, tandis que les quatre autres (France, Lettonie, Portugal et Italie) sont moins performants.



Source: DESI 2020, European Commission.

Il est important de souligner que les résultats de DESI 2020 ne semblent pas confirmer une correspondance linéaire entre le PIB du pays et la diffusion des compétences numériques. En effet, l'Espagne, par exemple, classée 5e économie de l'UE, n'est que 10e dans l'indice de l'économie et de la société numériques. Plusieurs initiatives ont récemment été introduites dans certains des pays qui composent le consortium afin d'améliorer la numérisation de l'économie et de la société. En tant que pays leader de l'UE pour la préparation à la 5G, l'Allemagne a pris plusieurs mesures pour faire progresser la numérisation, notamment des

initiatives dans les domaines de la sécurité informatique, des supercalculateurs, de l'IA et de la blockchain. De nombreux efforts ont été déployés pour faciliter la numérisation des entreprises et des services publics en France, notamment des efforts visant à mettre en place un écosystème pour soutenir les start-ups technologiques. Le gouvernement italien a adopté " Italia 2025 " en décembre 2020, un plan sur 5 ans qui place l'innovation et la numérisation au centre d'un " processus de transformation radicale et structurelle du pays ". Dans les années à venir, ces initiatives - qui nécessitent une mise en œuvre soutenue dans le temps et sont également susceptibles de nécessiter des investissements - pourraient se traduire par une progression de ces États membres sur le DESI.

L'impact de la pandémie COVID-19 sur le niveau des compétences numériques et en matière de cybersécurité est un autre aspect important. Bien qu'un tel lien entre l'urgence sanitaire et le nombre de cyberattaques ne soit pas immédiatement clair pour le grand public, en réalité, la première a entraîné une augmentation de la seconde Les cybercriminels sont très flexibles lorsqu'il s'agit d'exploiter de nouveaux événements, comme nous l'avons vu avec la récente urgence sanitaire. En 2020, de nombreuses entreprises ont adopté de nouvelles stratégies numériques (comme le travail à distance) et se sont ouvertes par inadvertance à toute une série de nouveaux vecteurs d'attaque que les criminels se sont empressés d'exploiter. Entre autres, l'événement inattendu COVID-19 a été utilisé pour diffuser des tentatives de logiciels malveillants : par exemple, des courriels au nom de l'Organisation mondiale de la santé, indiquant que la pièce jointe contient les dernières informations sur la pandémie ; des liens vers des graphiques montrant la propagation du virus, dont la fonctionnalité était de voler les données des utilisateurs ; des courriels malveillants adressés à des établissements de santé concernant la livraison d'équipements de protection COVID-19 et bien d'autres.

Pour réaliser ce rapport de recherche du consortium, nous avons utilisé la recherche documentaire, qui a consisté à localiser et à collecter des données, des publications, des

rapports de l'UE, des législations nationales et européennes en suivant les références fournies dans le rapport. Plus précisément, l'étude a exploré la question de la culture numérique et de la cybersécurité dans les différents contextes nationaux, en mettant l'accent sur la formation des enseignants de l'EFP. En outre, ce rapport de recherche du consortium met en lumière certains des acteurs clés engagés dans le secteur de la cybersécurité, notamment les organismes nationaux et l'Agence de l'Union européenne pour la cybersécurité (ENISA), qui coopère avec les États membres et les organismes de l'UE et aide l'Europe à se préparer aux futurs cyberdéfis.

1. Recherche documentaire sur les compétences numériques des enseignants de l'EFP

Allemagne:

- Le rapport sur les données de l'EFP (2019) élaboré par l'Institut fédéral allemand pour l'enseignement et la formation professionnels (BIBB), a inclus la "numérisation" parmi les 3 tendances clés pour les professions de la formation professionnelle et l'EFP en général.

- Plus précisément, le rapport indique que "la numérisation va renforcer les changements structurels du marché du travail", ce qui rend nécessaire une modification des capacités de formation dans les domaines concernés. Par conséquent, à l'avenir, le marché du travail allemand et européen aura particulièrement besoin de spécialistes professionnels hautement qualifiés.

- Comme le souligne la résolution de la Conférence permanente des ministres de l'éducation et des affaires culturelles (2016-2017) - "Bildung in der digitalen Welt" (L'éducation dans le monde numérique) - dans 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.

- Le ministère fédéral de l'éducation et de la recherche (BMBF) et l'Institut fédéral pour l'enseignement et la formation professionnels (BIBB) abordent depuis 2015 les questions de recherche, de développement et de pratique, liées à la transformation numérique du monde du travail et de l'enseignement et de la formation professionnels.

Irlande:

- L'une des principales stratégies de l'Irlande concernant les compétences numériques des éducateurs de la FEP est la stratégie numérique nationale qui a été lancée en juillet 2013.
- La stratégie se concentre sur l'engagement numérique et souligne comment l'Irlande peut bénéficier d'une société engagée numériquement.
- La stratégie définit une vision claire de l'avancement numérique de l'Irlande par la mise en œuvre d'un certain nombre d'actions pratiques pour aider à augmenter le nombre de citoyens et d'entreprises s'engageant en ligne par le biais de l'industrie et des entreprises, de la formation des citoyens, des écoles et de l'éducation.
- En ce qui concerne les compétences numériques des éducateurs de l'enseignement et de la formation professionnels (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.
- De nombreux éducateurs ont déclaré qu'ils pensaient que les appareils numériques pouvaient "provoquer des distractions" chez les apprenants. Au contraire, de nombreux éducateurs pensent que l'utilisation d'appareils numériques et d'applications dans le cadre d'activités d'apprentissage peut renforcer l'autonomie des apprenants et les aider à acquérir des compétences de vie du 21e siècle, comme payer des factures en ligne ou postuler à un emploi.

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.

Italie:

- Dans le domaine de l'éducation, les actions ont été menées principalement par le biais de la mise en œuvre du Plan national d'école numérique (Piano Nazionale Scuola Digitale- PNSD).
- Il s'agit du document d'orientation du ministère de l'éducation, de l'université et de la recherche pour le lancement d'une stratégie globale d'innovation 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).
- À cet égard, des projets ont été mis en œuvre pour les instituts d'enseignement technique et de formation professionnelle postsecondaires (Istituti Tecnici Superiori - ITS), avec un accent particulier sur le renforcement des compétences des étudiants.
- Par exemple, en 2019, le projet "ITS 4.0" a impliqué plus de 1.170 étudiants des ITS et environ 130 entreprises partenaires dans 106 projets d'innovation technologique axés sur des technologies telles que l'impression 3D, la réalité virtuelle et le big data.

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. Parmi ses mesures spécifiques, les mesures suivantes peuvent être mises en avant dans le cadre de cette analyse :

- mettre à jour le catalogue national des qualifications professionnelles en termes de compétences et de formation aux TIC, et inclure cette mise à jour dans les offres de formation qui accréditent les qualifications professionnelles ;
- maximiser l'efficacité de la gestion et de l'allocation des fonds de formation pour la formation continue en TIC, tant pour les travailleurs du secteur privé que pour ceux du secteur public, en accordant une attention particulière à l'utilisation de plateformes de formation virtuelle en ligne ;
- affecter une partie des ressources disponibles pour la FPC à l'acquisition et à la mise à niveau des compétences numériques des professionnels des TIC ;
- réajuster la formation professionnelle liée aux TIC en incluant, entre autres actions, des cours de spécialisation dans la mission d'enseignement ;
- promouvoir une amélioration de l'offre universitaire visant à former des professionnels des TIC par leur adaptation aux besoins du marché, en envisageant de nouveaux profils professionnels dans le domaine des TIC et en augmentant l'efficacité du système..

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.

- L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a constaté une augmentation très rapide du niveau de la cybermenace en France. Poursuivant une trajectoire initiée en 2019, le nombre de cyber-attaques a explosé : le nombre de victimes a ainsi été multiplié par 4 en un an.
- Les statistiques montrent que la densité des formations informatiques 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.
- Des études complémentaires pour voir la différence pourraient être menées ultérieurement par les bureaux régionaux ou les CNF s en fonction de leurs propres politiques locales ou régionales d'éducation numérique.

Lettonie:

- Bien qu'il y ait actuellement un manque d'études de recherche et de données en Lettonie sur la cybersécurité et les autres compétences numériques des éducateurs de l'EFP et d'autres établissements d'enseignement, il est évident que la transition vers l'enseignement à distance, en raison des crises du covid-19, s'est avérée être un défi majeur pour de nombreux enseignants.
- En ce qui concerne les stratégies nationales, les documents de planification de la nouvelle période budgétaire (2021-2027) soulignent les aspects suivants :

o Le développement des compétences numériques dans le secteur de l'éducation (Lignes directrices pour la transformation numérique 2021-2027) - il prévoit le développement des compétences numériques des éducateurs et des responsables d'établissements d'enseignement, le développement et l'utilisation des compétences numériques dans le processus éducatif, ainsi que le soutien au développement des compétences numériques des adultes employés ;

o Le développement des compétences numériques est inclus dans le programme de développement des compétences professionnelles des éducateurs (Education Development

Guidelines 2021- 2027). 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 d'euros) ;

o 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") ;

o le développement des compétences numériques de la société en général (lignes directrices pour le développement de l'éducation 2021-2027, lignes directrices pour la transformation numérique 2021-2027), car les compétences numériques sont désormais assimilées à la littératie et à la numératie en termes d'importance et, au moins au niveau de base, elles sont nécessaires à tous, quel que soit le domaine d'activité (compétences numériques = compétences transversales). Il convient de prendre des mesures pour éduquer la population aux compétences numériques de base, à l'éducation aux médias et à la maîtrise de l'information, qui englobent l'ensemble des compétences de base, y compris les cybercompétences ;

L'attention qui a été accordée à l'indice DESI susmentionné dans l'introduction de ce rapport de recherche se justifie par la précision avec laquelle il décrit l'état de l'art et le caractère divergent selon les différents pays européens. Une telle précision est également confirmée par les rapports nationaux uniques concernant les compétences numériques des éducateurs de l'EFP.

Nous pensons qu'il est particulièrement utile de comparer les deux extrêmes du consortium, afin de comprendre comment les différents degrés de compétences numériques affectent la population nationale, et plus particulièrement les éducateurs de l'EFP. Nous considérerons tout d'abord l'Irlande, classée au 6e rang du classement DESI.

Selon l'Office central des statistiques (CSO) irlandais, en 2018, 89 % des ménages disposent d'un

d'un accès à Internet à domicile. En outre, plus de 30 % de toutes les données de l'UE sont hébergées en Irlande, car bon nombre des plus grandes entreprises technologiques du monde ont leur siège en Europe. Si l'on combine ces deux statistiques, il va sans dire qu'il est crucial de veiller à ce que l'Irlande soit un pays prêt pour la cybersécurité. Tout au long de ce rapport national, il sera fait référence à la législation clé qui existe en Irlande concernant la culture numérique et la cybersécurité.
cybersécurité. Alors que le monde continue de s'adapter à "vivre avec COVID-19", il est nécessaire de s'assurer que le paysage de la lutte contre la cybercriminalité et les modèles de meilleures pratiques continuent d'influencer les politiques et les pratiques.

L'une des stratégies clés de l'Irlande concernant les compétences numériques est la stratégie numérique nationale qui a été lancée en juillet 2013. La stratégie se concentre sur l'engagement numérique et souligne comment l'Irlande peut bénéficier d'une société engagée numériquement. La stratégie définit une vision claire de l'avancement numérique de l'Irlande par la mise en œuvre d'un certain nombre d'actions pratiques pour aider à augmenter le nombre de citoyens et d'entreprises s'engageant en ligne par le biais de l'industrie et des entreprises, de la formation des citoyens, des écoles et de l'éducation. En 2021, la ministre de l'éducation, Norma Foley, a annoncé le développement d'une nouvelle stratégie numérique pour les écoles primaires. Cette stratégie sera principalement axée sur l'utilisation de la technologie numérique dans l'éducation et améliorera l'apprentissage en intégrant la technologie dans l'avenir. Dans l'espace de l'enseignement supérieur en Irlande, l'un des développements les plus notables est une feuille de route pour l'apprentissage numérique dans l'enseignement supérieur : 2015 - 2017 qui a été développée pour soutenir une "approche coordonnée et à plusieurs niveaux pour favoriser la culture numérique, les compétences et la confiance parmi les étudiants à tous les niveaux de l'éducation".

En ce qui concerne l'enseignement et la formation complémentaires, un ministère relativement nouveau de l'enseignement complémentaire et supérieur, de la recherche, de l'innovation et des sciences a été créé. Dans le cadre de la stratégie triennale de ce ministère, l'un des principaux domaines d'action concerne les compétences numériques, l'objectif étant de mettre en œuvre une nouvelle stratégie décennale visant à améliorer la littératie, la numératie et les compétences numériques. En outre, il s'agit de

la réforme de la formation professionnelle et l'investissement dans la promotion des compétences numériques. 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 les appareils numériques dans leur classe comme outil d'apprentissage et ceux qui ne le font pas.

-
- De nombreux éducateurs ont déclaré qu'ils pensaient que les appareils numériques pouvaient "provoquer des distractions" chez les apprenants. Cependant, au contraire, de nombreux éducateurs pensent que les appareils numériques et les applications dans les activités d'apprentissage peuvent responsabiliser les apprenants et les aider à s'engager dans les compétences de vie du 21e siècle, comme payer des factures en ligne/candidater pour des emplois. Une dernière stratégie intergouvernementale qui mérite d'être notée du point de vue irlandais est l'initiative 2018 Future Jobs Ireland, qui met l'accent sur une philosophie d'apprentissage tout au long de la vie. Parmi ses cinq thèmes clés, le deuxième se concentre sur "l'innovation et la technologie, y compris la préparation de la transition vers l'économie numérique". Cette stratégie est au cœur des discussions concernant la nécessité de poursuivre les recherches et les investissements dans le domaine des compétences numériques.
-
- Cette compréhension et cette appréciation communes des moyens numériques

  confirment l'Irlande comme un pays leader en termes d'intégration de la technologie

numérique. Cette intégration est, entre autres, l'un des principaux problèmes du contexte italien.

- En Italie, moins de la moitié de la population possède des compétences numériques de base et le pourcentage de spécialistes en TIC, qui ne représente que 1 % des diplômés italiens, est toujours inférieur à la moyenne européenne, même s'il a augmenté ces dernières années. En outre, les données de l'enquête internationale de l'OCDE sur l'enseignement et l'apprentissage (2013) placent l'Italie au premier rang pour les besoins de formation en TIC de ses enseignants. Au moins 36 % des enseignants italiens ont déclaré qu'ils n'étaient pas suffisamment préparés à l'enseignement numérique, contre une moyenne de 17 % pour l'OCDE, ce qui montre qu'une formation spécifique est nécessaire.
-
- Ces dernières années, en termes de réponse politique, l'Italie a intégré des mesures relatives aux compétences numériques dans plusieurs stratégies sectorielles. Dans le domaine de l'éducation, les actions ont été menées principalement par la mise en œuvre du Plan national d'école numérique (Piano Nazionale Scuola Digitale - PNSD), qui est le document d'orientation du ministère de l'éducation, de l'université et de la recherche pour le lancement d'une stratégie globale d'innovation pour l'école italienne et pour un nouveau positionnement de son système éducatif dans l'ère numérique. C'est un pilier fondamental de La Buona Scuola (loi 107/2015), une vision opérationnelle qui reflète la position du gouvernement par rapport aux défis d'innovation les plus importants du système public et, au centre de cette vision, il y a l'innovation du système scolaire et les opportunités de l'éducation numérique. Les domaines d'intervention identifiés par le PNSD sont : l'accès, les espaces et les environnements d'apprentissage, l'administration numérique, l'identité numérique, les compétences des étudiants, l'entrepreneuriat et le marché du travail, le contenu numérique, la formation du personnel. Concernant ce dernier point, le PNSD soutient que la formation des enseignants doit être centrée sur

l'innovation pédagogique, en prenant en compte les technologies numériques comme support à la mise en œuvre de nouveaux paradigmes éducatifs et à la planification opérationnelle des activités. Les objectifs de cette action sont :

● Renforcer la préparation du personnel dans le domaine des compétences numériques, en touchant l'ensemble de la communauté scolaire ;
● Promouvoir le lien entre l'innovation pédagogique et les technologies numériques ;
● Développer des normes efficaces, durables et continues dans le temps pour la formation à l'innovation pédagogique ;
● Renforcer la formation à l'innovation pédagogique à tous les niveaux (initial, entrant, en service).

In order pour favoriser la formation des enseignants sur les sujets informatiques, un protocole d'accord a été signé avec des organismes de formation et des ressources financières ont été fournies pour faciliter la participation aux cours, comme :

● Le protocole d'accord n°. 785 du 22 janvier 2021 entre le ministère de l'Éducation et Cisco " Innover et améliorer les compétences numériques à l'école " et le programme de formation " Enseignants connectés et sûrs ".
● Le protocole d'accord n°. 4 du 28 octobre 2020 entre le ministère de l'Éducation et S.O.S. The Telefono Azzurro Onlus pour la réalisation d'activités éducatives et de formation conjointes visant à promouvoir l'éducation à la citoyenneté numérique et l'utilisation consciente des technologies numériques, des médias sociaux et des cours de formation pour les enseignants.

Jusqu'à présent, 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). À cet égard, des projets ont été mis en œuvre pour les instituts d'enseignement technique et de formation professionnelle postsecondaires (Istituti Tecnici Superiori - ITS), avec un accent particulier sur le renforcement des compétences des étudiants. Par exemple, en 2019, le projet "ITS 4.0" a impliqué plus de 1.170 étudiants des ITS et environ 130 entreprises partenaires dans 106 projets d'innovation technologique axés sur des technologies telles que l'impression 3D, la réalité virtuelle et le big data.

Un autre outil qui contribuera à l'acquisition de compétences numériques est inclus dans le plan national de relance et de résilience (Piano Nazionale di Ripresa e Resilienza - PNRR), qui fait partie du programme Next Generation EU, un paquet de 750 milliards d'euros, dont près de la moitié est constituée de subventions, décidé par l'Union européenne en réponse à la crise de la pandémie. Le PNRR va promouvoir le développement des compétences numériques du personnel scolaire afin d'encourager une approche accessible, inclusive et intelligente de l'éducation numérique. L'objectif principal est la création d'un écosystème de compétences numériques, capable d'accélérer la transformation numérique de l'organisation scolaire et des processus d'apprentissage et d'enseignement, conformément au cadre de référence européen pour les compétences numériques DigComp 2.1 (pour les élèves) et DigCompEdu (pour les enseignants). La mise en œuvre de cette ligne d'action est assurée par le ministère de l'éducation et impliquera environ 650 000 personnes, y compris les enseignants et le personnel scolaire, et plus de 8 000 établissements d'enseignement. Le gouvernement a l'intention de renforcer l'enseignement professionnel, en particulier le système de formation professionnelle tertiaire (ITS) et l'enseignement STEM, avec une forte priorité sur l'égalité des sexes..

Les contextes susmentionnés représentent deux contextes nationaux différents. Afin d'avoir une indication plus proche du cadre général européen, il peut être utile d'analyser le paysage des compétences numériques en France, un pays qui, sur l'échelle DESI, est très proche de la moyenne européenne et la suit immédiatement. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a constaté une augmentation très rapide du niveau de la cybermenace en France. Poursuivant une trajectoire initiée en 2019, le nombre de cyber-attaques a explosé : le nombre de victimes a ainsi été multiplié par 4 en un an. Ce constat est particulièrement inquiétant, surtout dans un contexte où toute cyber-attaque est susceptible d'avoir un impact exacerbé en raison de la crise sanitaire. La méconnaissance des cyber-risques, le manque de maîtrise des systèmes d'information, le non-respect des mesures d'hygiène informatique, la pénurie d'experts en cybersécurité et, dans une certaine mesure, l'augmentation de la surface d'attaque due à la généralisation du télétravail, sont autant de faiblesses exploitées par les cybercriminels. Les campagnes d'attaques qui ont touché la France en 2020 ont réussi à perturber de nombreuses entreprises et à causer des pertes financières importantes. Le recours massif à des services numériques externalisés, souvent moins sécurisés, est une pratique répandue que les attaquants ne manquent pas d'exploiter. Les statistiques montrent que la densité des formations informatiques varie d'une région francophone à l'autre. Il y a plusieurs raisons à cela. Parmi elles, la plus importante est sans doute liée aux institutions académiques et à leurs gouvernements. Des études complémentaires pour voir la différence pourraient être menées ultérieurement par les bureaux régionaux ou les CNF en fonction de leurs propres politiques locales ou régionales d'éducation numérique. Les statistiques de formation montrent que les besoins thématiques qui ont fait l'objet d'ateliers de formation varient également d'une région à l'autre. La fréquence thématique en ce sens dépend également de facteurs endogènes liés à la demande et à l'offre en fonction des besoins et des niveaux d'avancement dans les domaines des TIC/E et de la FOAD des partenaires locaux.

2. Recherche documentaire sur les principaux problèmes de sécurité numérique dans les pays partenaires.

Allemagne

- Pour analyser le contexte spécifique de l'Allemagne et en tirer une analyse des besoins, il est particulièrement important d'examiner le Baromètre numérique 2020, une enquête en ligne représentative des citoyens privés sur la cybersécurité, menée conjointement par le BSI et la Commission de prévention de la criminalité de l'État allemand et de la police fédérale.
- Ces dernières années, dans le paysage allemand et européen, la cybercriminalité a été la principale cause des récentes cyberattaques. Le rapport 2020 du BSI a confirmé les fuites de données et les vulnérabilités critiques découvertes dans les produits logiciels et matériels. Cette recherche a également remarqué une augmentation des cybercrimes de masse ciblant des citoyens privés, des entreprises commerciales et d'autres institutions à l'aide de logiciels malveillants.
- La vulnérabilité la plus courante exploitée par les logiciels malveillants est une vulnérabilité du système hôte. Dans le cas de produits logiciels ou matériels, les vulnérabilités peuvent se trouver dans les passerelles, comme celles qui fonctionnent entre les bureaux ou les réseaux de production, ou elles peuvent être causées par une erreur humaine dans le cadre de l'ingénierie sociale.
- Ce degré de numérisation n'est pas sans risques et dangers. Un répondant sur quatre a déclaré avoir été victime de cybercriminalité au cours de l'année écoulée. Le taux global de cybercriminalité en 2020 reste constant. Les achats en ligne et l'accès de tiers à des comptes en ligne sont les types de fraude les plus courants qui touchent les victimes (44%) et (30%), respectivement.

Malgré ces résultats, deux tiers des personnes interrogées ont exprimé le souhait d'obtenir davantage d'informations sur la prévention du vol de données (66%). Les conseils recherchés consistent le plus souvent en des astuces pratiques telles que les moyens de garantir des mots de passe sûrs pour plusieurs comptes en ligne (59 %), suivis par des conseils sur les logiciels les mieux adaptés à la protection des comptes en ligne (52 %) et des conseils sur les avantages et les inconvénients des gestionnaires de mots de passe (49 %).

Irlande :

- Les menaces de cybersécurité en Irlande continuent d'augmenter, la dernière attaque de cybersécurité ayant eu lieu en 2021 sur l'Ireland Health Service Executive (HSE) qui a et continue d'avoir des effets dévastateurs sur le système de santé irlandais.
- L'Irlande abrite plus de 30 % des données de l'UE en raison du nombre de centres de cybersécurité ayant leur siège dans le pays. Bien que cette situation offre de nombreuses possibilités, elle entraîne également une augmentation du niveau de menace de la cybercriminalité. L'Irlande étant une démocratie libérale ouverte, elle est considérée comme particulièrement vulnérable aux attaques de type "hack and leak".
- La deuxième stratégie nationale de cybersécurité 2019 - 2024 de l'Irlande a été lancée dans le but d'améliorer la préparation du pays en matière de cybersécurité. Les principaux objectifs de cette stratégie sont les suivants

o Assurer la préparation de l'Irlande en matière de cybersécurité et répondre aux incidents de cybersécurité, y compris ceux concernant la sécurité nationale, et les gérer,

o Protéger et gérer toute perturbation des services impliquant des infrastructures nationales critiques à la suite de cyberattaques,

o poursuivre la croissance et le développement du secteur de la cybersécurité en Irlande et être prêt pour la cybernétique,

o Mettre en œuvre dans les entreprises irlandaises les meilleures technologies et mesures disponibles au niveau international,

o Sensibiliser et développer les compétences des organisations et des particuliers autour de la cybersécurité.

- En 2018, un plan d'action pour la sécurité en ligne a été lancé et contient vingt-cinq actions dans le cadre de cinq objectifs principaux centrés sur la légalisation des infractions pénales concernant la cybercriminalité, le retrait du matériel illégal et nuisible et l'incitation à la sécurité en ligne.

Portugal

- Les principaux sujets de sécurité numérique à assurer sont

o Niveau de base

Identifier l'exposition de l'infrastructure et des applications de votre école dans l'environnement en ligne et adopter des mesures d'atténuation des risques (à la fois structurelles et comportementales) ;

Identifier et atténuer les vulnérabilités ;

Identifier les informations personnelles sur Internet qui peuvent être utilisées pour une attaque;

Acquérir un ensemble de comportements appropriés dans l'utilisation du cyberespace ;

o Niveaux intermédiaire et avancé :

Programmation de la sécurité Environnements techniques

Ingénierie sociale

Exploration des sources de données ouvertes

Réseaux sans fil

Cryptage et mots de passe

Italie :

- Le problème de sécurité le plus répandu au cours des trois dernières années en Italie est le phishing de mots de passe, indiqué par 48% des managers italiens, contre 36% des managers

européens. En outre, 28% des managers italiens ont des problèmes liés à l'accès et à l'identité (en ligne avec le pourcentage européen), suivis par le problème des logiciels malveillants basés sur l'ingénierie sociale (24%).

- Par ailleurs, seuls 42 % des personnes âgées de 16 à 74 ans possèdent des compétences numériques de base et le pourcentage de diplômés en informatique et en TIC est très faible par rapport aux données européennes.
- Le gouvernement s'attaque aux compétences numériques dans "Italia 2025", une stratégie quinquennale pour l'innovation et la numérisation lancée en 2019. Cette stratégie comprend notamment "Digital Republic", une initiative promue et coordonnée par le ministère de l'innovation technologique et de la numérisation.
- Cette initiative vise à créer une alliance entre les organisations publiques et privées et les citoyens, et à les inviter à prendre des mesures concrètes pour promouvoir les compétences numériques. Elle se concentre sur trois lignes d'action :

o stimuler les compétences numériques de base ;

o promouvoir l'amélioration et le renouvellement des compétences de la main-d'œuvre ;

o développer les compétences en matière de TIC et de technologies émergentes.

- Une nouvelle étape sera franchie avec "Italia digitale 2026", qui fixe cinq objectifs ambitieux à atteindre dans les années à venir :

o Diffuser l'identité numérique, en veillant à ce qu'elle soit utilisée par 70 % de la population ;

o combler le déficit de compétences numériques, en veillant à ce qu'au moins 70 % de la population ait des compétences numériques

numérique ;

o Amener environ 75 % des AP italiennes à utiliser les services en nuage ;

o Atteindre au moins 80% des services publics essentiels fournis en ligne ;

o atteindre, en collaboration avec la Mise, 100% des familles et des entreprises italiennes avec des réseaux à très haut débit.

Espagne :

- La stratégie espagnole d'activation pour l'emploi 2017-20 vise à consolider la reprise économique en promouvant des programmes et des ressources de cybersécurité pour les institutions de formation professionnelle afin de relever les défis du marché du travail actuel et futur découlant de la mondialisation et de la numérisation. Il établit les mesures à mettre en œuvre, tant au niveau de l'État que des régions, par les services publics de l'emploi (SPE) ;
- En termes quantitatifs, l'un des objectifs est la formation aux compétences numériques d'au moins 225 000 jeunes : 75% en compétences de base et 25% en compétences numériques avancées, ce qui représente respectivement 40% et 38% de la population jeune de moins de 30 ans.

o soutien au démarrage de projets technologiques pour les jeunes femmes, en fournissant un consultant pour conseiller ces entrepreneurs sur leur plan d'affaires et en offrant des services de suivi ;

o des actions de formation spécifiques pour les jeunes femmes des zones rurales dans les technologies des TIC et les nouveaux secteurs d'avenir, en tirant parti des possibilités des nouvelles technologies et avec des formateurs et des tuteurs, y compris l'enseignement en ligne ;

o la promotion de l'esprit d'entreprise, du travail indépendant et des nouvelles possibilités d'emploi offertes par l'économie numérique et les différentes formules de l'économie sociale et de l'économie des plateformes numériques, dans le cadre des politiques d'activation de l'emploi ;

o l'amélioration de la visibilité des meilleures pratiques développées pour comprendre quels sont les principaux sujets de sécurité numérique.

- Programme opérationnel national sur l'emploi des jeunes (budget de 39 millions d'euros). À titre d'exemple, le programme comprend un parcours de formation sur la transformation numérique pour l'emploi.

- Le projet, mis en œuvre par EOI avec le partenariat de Google, vise à améliorer l'employabilité des jeunes qui ont abandonné l'école dès leur plus jeune âge, qui ont perdu leur emploi ou qui ont des difficultés à trouver leur premier emploi.

France :

- Les ministres de l'enseignement supérieur de la francophonie se sont réunis le 5 juin 2015 à Paris à l'initiative conjointe de la France, de l'OIF (Organisation internationale de la francophonie) et de l'AUF (Agence universitaire de la francophonie) pour examiner l'état et les perspectives du développement numérique de l'espace universitaire & de la formation professionnelle francophone.
- L'objectif principal de ce travail était de contribuer à l'élaboration d'une stratégie francophone de formation des formateurs dans le domaine de l'éducation numérique et d'évaluer les besoins et les attentes en matière de formation des groupes cibles concernés, puis de déterminer ce qui est nécessaire pour répondre à ces besoins et attentes, notamment en termes de services, de contenus et de compétences.
- Selon l'étude " Étude sur l'identification des besoins en formation tic/e dans les pays francophones du sud, 2016 ", Le nee.

Lettonie:

- Selon la stratégie nationale de cybersécurité 2019-202215, le cyberespace letton continue d'être confronté à des menaces de grande ampleur - hameçonnage, extorsion et logiciels malveillants, tentatives de piratage des systèmes, réseaux et sites web, attaques par déni de service (DoS) sur les systèmes d'information critiques ainsi que courriers électroniques frauduleux et campagnes d'ingénierie sociale visant à récupérer des données personnelles ou d'authentification pour discréditer une personne, une entreprise ou une institution spécifique ou pour commettre des crimes.

- En Europe comme en Lettonie, les incidents suivants sont devenus d'actualité : tentatives d'extorsion d'argent visant principalement des institutions financières ou des entreprises du secteur privé (les attaquants ont réalisé une série d'attaques à titre d'essai, menaçant de suspendre le fonctionnement des sites Web des entreprises ou d'autres ressources au moyen d'attaques pouvant atteindre 2 Tb/s).
- En 2021, la fraude, les logiciels malveillants et les vulnérabilités continuent d'être actifs - comptes WhatsApp volés grâce à des codes d'activation demandés par des comptes piratés de la liste de contacts d'une personne ; nouvelle vague d'e-mails de chantage (sextorsion) - menaçant de distribuer du matériel compromettant, si l'utilisateur de l'e-mail ne verse pas de rançon.
- L'année 2020 et ses changements globaux ont démontré que pour les éducateurs de l'EFP et d'autres établissements d'enseignement, il est important d'avoir des connaissances/compétences accrues sur la sécurité du travail à distance lors de l'organisation de cours en ligne et de l'utilisation d'outils numériques (e-mails, WhatsApp, plateforme d'apprentissage, etc.

Bien que le lien entre la pandémie de COVID-19 et le bilan des cyberattaques ne soit pas immédiatement clair pour le grand public, en réalité, la première a entraîné une augmentation de la seconde. Les cybercriminels sont très souples lorsqu'il s'agit d'exploiter de nouveaux événements, comme nous l'avons vu avec la récente urgence sanitaire. Le grand nombre d'entreprises qui ont adopté de nouvelles stratégies numériques cette année (par exemple, le travail à distance) s'est ouvert par inadvertance à une série de nouveaux vecteurs d'attaque que les criminels se sont empressés d'exploiter.

Les bureaux nationaux offrent une perspective à multiples facettes sur les principales questions liées au numérique et à la cybersécurité. Alors que l'enseignement à distance devient la

nouvelle normalité, les cybercriminels trouvent de nouveaux moyens d'exploiter des techniques telles que le phishing, les ransomwares, l'ingénierie sociale, etc. pour lancer leurs attaques. Voici quelques-uns des risques les plus critiques rencontrés.

1. Accès à distance sécurisé

À mesure que l'enseignement à distance prend le relais de l'enseignement physique, les élèves et les enseignants ont besoin d'accéder à des outils d'apprentissage en ligne principalement situés dans le cloud, c'est-à-dire à des applications de partage de fichiers, à des courriers électroniques, à des applications, et ils doivent parfois accéder à distance aux ressources du réseau scolaire. Si l'accès à distance n'est pas sécurisé, les pirates peuvent pénétrer dans le système et prendre le contrôle de l'ensemble du réseau.

2. Accès aux données sensibles

Les établissements d'enseignement contiennent un trésor de données sensibles qui peuvent être vendues sur le dark web. Les données personnelles des étudiants, des enseignants, des anciens élèves et du personnel administratif, ainsi que les données sensibles relatives à la recherche et à la propriété intellectuelle d'une école, peuvent constituer un véritable trésor qu'un pirate peut vendre ou rançonner. Il est donc essentiel de mettre en place un accès basé sur l'identité, permettant aux utilisateurs autorisés d'accéder uniquement aux ressources dont ils ont besoin pour faire leur travail.

3. Logiciels malveillants

Le passage à l'enseignement à distance signifie que de nombreux appareils connectés au réseau de l'école sont des BYOD (Bring Your Own Device). Il est difficile de savoir si les appareils et les applications utilisés sont correctement mis à jour avec des correctifs et si l'antivirus lui-même est à jour. À moins que ces appareils distants ne se connectent via un VPN, vous devez vous assurer qu'ils sont sécurisés avant qu'ils puissent accéder aux ressources du réseau de

formation. Il est important de déployer des fonctionnalités avancées de protection du Web qui peuvent identifier et bloquer les dernières menaces Web.

4. Phishing

Les attaques d'ingénierie sociale et de phishing sont des risques majeurs de cybersécurité pour les centres de formation français. Les formateurs et les enseignants ou les membres du personnel qui sont amenés à cliquer sur des liens malveillants peuvent permettre aux cybercriminels d'accéder au réseau de l'école et à ses précieuses ressources. La meilleure façon de contrer les attaques d'ingénierie sociale et de phishing est de sensibiliser et de former les utilisateurs. Former et tester vos utilisateurs à l'aide d'attaques simulées contribuera à instaurer une culture positive de sensibilisation à la sécurité et les rendra moins vulnérables aux diverses escroqueries en ligne.

5. Fraude

En ce qui concerne la fraude, l'année 2020 a été signalée comme étant très intensive, y compris les attaques d'ingénierie sociale. Parmi les tentatives de fraude les plus actives, on trouve les campagnes d'extorsion, où les pirates prétendent avoir piraté l'appareil d'un utilisateur et obtenu du matériel compromettant pour lequel une rançon a été fixée ; les loteries frauduleuses au nom des marques connues, offrant de gagner les derniers smartphones ou d'autres prix de valeur.

Une nouvelle tendance a été observée : les e-mails d'extorsion avec menace de fuite de données. À de nombreuses reprises, des entreprises ont été visées. Des publicités trompeuses sur les médias sociaux - utilisant les noms de personnes célèbres à leur insu, invitaient les internautes à investir dans les crypto-monnaies. Les escrocs ont également passé des appels téléphoniques et tenté de persuader les gens d'investir. Dans certains cas, des tentatives frauduleuses répétées ont été observées, où les victimes de fraude financière se sont vu proposer de l'aide pour récupérer leurs ressources perdues.

Arnaques téléphoniques - en falsifiant les numéros de téléphone de différents établissements de crédit et en se faisant passer pour des représentants de banques, les escrocs, profitant de la méconnaissance du public des méthodes d'authentification supplémentaires, ont escroqué les ressources financières de plusieurs milliers d'utilisateurs, causant des pertes totales de plusieurs centaines de milliers de dollars aux établissements de crédit lettons. Adaptation des pirates à la nécessité de commencer le travail à distance - compte tenu de la nécessité pour les entreprises de passer rapidement à des conditions de travail à distance et de mettre en œuvre la circulation des documents électroniques, les pirates ont profité de la situation pour faire de la publicité. Par exemple, un certain nombre de comptables d'entreprises ont reçu des courriels au nom du directeur ou d'un autre employé pour effectuer un paiement urgent ou modifier le compte de paie.

Interférence dans la correspondance commerciale des entreprises - en compromettant les e-mails des entreprises ou de leurs partenaires de collaboration, les pirates ont pu choisir le moment opportun pour envoyer à l'une des parties une facture avec un compte modifié.

De nombreux internautes ont été la cible de messages d'escroquerie contenant des liens raccourcis (ej.uz), utilisés pour masquer la destination réelle du lien, au nom des institutions de l'État concernant l'état d'urgence et la situation épidémiologique du pays.

Fausses boutiques en ligne - une activité particulièrement élevée a été observée pendant la période des fêtes de fin d'année au moyen d'annonces sur les médias sociaux et en raison des restrictions covid-19 qui ont obligé les entreprises à vendre leurs produits en ligne.

Il peut être utile d'utiliser certaines données rapportées par les rapports nationaux. Par exemple, en France, les risques numériques sont très présents dans les représentations des jeunes enseignants, qui relaient facilement le discours médiatique. Les trois risques auxquels les enseignants se sentent le plus personnellement confrontés sont les risques techniques (66,20%), éthiques et juridiques (55,80%) et informationnels (54,70%). Les risques psycho-sociaux, cognitifs et socio-économiques semblent moins les inquiéter. Il existe un décalage

systématique entre les représentations des risques pour eux-mêmes par rapport à celles pour les élèves. En effet, les trois risques auxquels les enseignants estiment que leurs élèves sont le plus confrontés sont les risques psychosociaux (69,95%), informationnels (70,75%) et techniques (62,80%). Les enseignants ressentent donc la même vulnérabilité que leurs élèves face aux risques techniques, mais considèrent que leurs élèves sont plus exposés aux problèmes liés au harcèlement ou aux fausses informations notamment. L'amplification des risques pour les élèves peut s'expliquer par le fait que les enseignants les perçoivent comme très vulnérables. Une enseignante stagiaire a décrit ses élèves de quatrième année comme étant très vulnérables, assez naïfs, pas forcément conscients du danger potentiel des réseaux.

Le rapport de l'Office fédéral allemand de la sécurité de l'information (BSI) indique que plusieurs campagnes ont exploité la confusion et la peur créées par COVID-19, notamment des campagnes de logiciels malveillants et de phishing, des fraudes aux PDG et des escroqueries. En outre, le BSI a déclaré que ces événements ont pu augmenter les chances de succès de ces attaques en raison des peurs, des inquiétudes et des insécurités associées à de tels événements. Ces dernières années, dans le paysage allemand et européen, la cybercriminalité a été la principale cause des récentes cyberattaques. Pour analyser le contexte spécifique de l'Allemagne et en tirer une analyse des besoins, il est particulièrement important d'examiner le Baromètre numérique 2020, une enquête en ligne représentative des citoyens sur la cybersécurité, menée conjointement par le BSI et la Commission de prévention de la criminalité de l'État et de la police fédérale allemande. La transition numérique façonne activement notre vie quotidienne, des achats en ligne aux wearables (tels que les brassards de suivi de la condition physique, les smartwatches ou les lunettes intelligentes), en passant par les nouveaux systèmes de paiement et d'identification.

Toutefois, ce degré de numérisation n'est pas sans risques et dangers. Un répondant sur quatre a déclaré avoir été victime de cybercriminalité au cours de l'année écoulée. Le taux global de

cybercriminalité en 2020 reste constant. Les achats en ligne et l'accès de tiers à des comptes en ligne sont les types de fraude les plus courants qui touchent les victimes (44%) et (30%), respectivement. La plupart des personnes interrogées dans le cadre de l'enquête connaissent les récentes recommandations en matière de prévention de la cybercriminalité. Ces recommandations ne sont généralement suivies que lorsque cela a du sens pour la personne qui les applique (41 %) ou qui vient d'apprendre l'existence d'un conseil particulier (39 %). Les recherches montrent que les personnes qui ont déjà été victimes à plusieurs reprises sont plus susceptibles de ne tenir compte des conseils que lorsqu'un problème survient (33 %), même si elles en avaient déjà connaissance. Finalement, malgré ces résultats, deux tiers des personnes interrogées ont exprimé le souhait d'obtenir davantage d'informations sur la prévention du vol de données (66%). Les conseils recherchés consistent le plus souvent en des astuces pratiques telles que les moyens de garantir des mots de passe sûrs pour plusieurs comptes en ligne (59 %), suivis par des conseils sur les logiciels les mieux adaptés à la protection des comptes en ligne (52 %) et des conseils sur les avantages et les inconvénients des gestionnaires de mots de passe (49 %).

Enfin, une autre perspective importante est offerte par l'Irlande et les menaces de cybersécurité survenues en 2021. Une attaque massive et coordonnée a débuté en mai 2021, a perturbé le service de santé et les systèmes informatiques dans tout le pays, a volé les données personnelles d'un pourcentage élevé de patients et continue d'exiger une rançon pour la restitution des données. En réponse, le Health Service Executive (HSE) a dû fermer les systèmes informatiques des hôpitaux et des services de santé pour se protéger contre tout nouveau vol de données. De nombreux services ont été interrompus et des informations personnelles et médicales ont été divulguées. Toutefois, il convient de noter que rien ne permet d'affirmer que d'autres escroqueries impliquant des informations personnelles ont eu lieu. L'Irlande abrite plus de 30 % des données de l'UE en raison du nombre de centres de cybersécurité ayant leur siège dans le pays. Bien que cette situation offre de nombreuses possibilités, elle entraîne également

un niveau accru de menace de cybercriminalité. L'Irlande étant une démocratie libérale ouverte, elle est considérée comme particulièrement vulnérable aux attaques de type "hack and leak". En général, ces attaques sont considérées comme ayant une motivation politique et sont centrées sur la désinformation et les "fake news" utilisées pour tenter de déstabiliser l'État.

De nombreuses personnes impliquées dans le secteur de la cybersécurité appellent à une augmentation des investissements dans les organismes publics tels que le Centre national de cybersécurité (NCSC) en Irlande. Les autres menaces/risques qui continuent de prévaloir sont les risques posés aux infrastructures nationales critiques (CNI), aux systèmes et aux données du secteur public, qui ont été brièvement décrits dans les paragraphes précédents. Les nouveaux problèmes qui commencent à émerger sont ceux liés au déploiement des technologies 5G. Bien que cela donne lieu à de nouvelles technologies et de nouveaux services, la cybersécurité doit être au premier plan de la réflexion alors que de nombreux pays commencent à s'adapter.

En dehors d'une perspective nationale et commerciale, les crimes liés à la cybersécurité continuent de se produire de manière prolifique au quotidien chez le citoyen moyen. Ils ne sont souvent pas signalés aux forces de l'ordre, seuls cinq pour cent des cybercrimes auraient été signalés à la police en Irlande en 2019. En outre, un rapport 2019 commandé par Microsoft en Irlande constate que les employés sont toujours considérés comme le "maillon faible" du système de sécurité en raison du manque de formation à la sécurité, de la mauvaise gestion des mots de passe, de l'utilisation d'appareils personnels avec des données liées au travail et des violations potentielles du règlement général de l'UE sur la protection des données.

3. Meilleures pratiques en matière de programmes et de ressources de cybersécurité pour les établissements d'enseignement et de formation professionnels dans l'Union européenne et dans chaque pays partenaire.

Comme spécifié dans l'introduction, le projet Cyber.EU.VET implique un consortium multiforme et diversifié. En ce qui concerne les compétences numériques et de cybersécurité, les pays partenaires du consortium présentent des degrés d'efficacité différents, comme le décrit parfaitement l'indice DESI.

L'analyse académique et l'évaluation des bonnes pratiques faisaient partie intégrante des travaux de recherche menés au niveau national par chaque partenaire du consortium du projet. Cette recherche avait pour ligne directrice commune une analyse des besoins en matière d'EFP au niveau local et national. En réalisant ce travail, les sept partenaires nationaux ont partagé certaines difficultés liées à la recherche d'initiatives de formation et de cybersécurité spécifiquement conçues pour les enseignants de l'EFP. Si cela a rendu la tâche assez difficile, cela a aussi montré encore plus clairement l'importance et la nécessité de développer des projets dans ce domaine. Elle a ensuite confirmé l'esprit extrêmement novateur du projet CYBER.EU.VET. Voici un recueil des bonnes pratiques les plus pertinentes trouvées par chaque partenaire.

3.1 Allemagne - Initiative VET 4.0

VET 4.0 est une initiative-cadre, développée en collaboration par le ministère fédéral de l'éducation et de la recherche (BMBF) et l'Institut fédéral de l'enseignement et de la formation

professionnels (BIBB) depuis 2016, qui a rassemblé un large éventail de projets au sein de trois piliers principaux. Le pilier 2 de cette initiative globale (qui est toujours en cours) est entièrement consacré à la "littératie numérique/compétence médiatique" et vise à définir les compétences médiatiques, qui devraient être considérées comme une condition d'entrée et comme une compétence clé dans toutes les professions de la formation professionnelle (pour les apprentis, les enseignants et les formateurs). Des programmes de financement visant à mieux équiper les centres de formation et à soutenir les petites et moyennes entreprises (PME) dans la perspective de la numérisation complètent cette approche de promotion des compétences médiatiques dans l'EFP. Grâce au programme spécial de numérisation ÜBS (71), le BMBF et le BIBB contribuent à accélérer la numérisation des processus de formation des apprentis dans le cadre de la " formation professionnelle 4.0 ". Le programme spécial se compose de deux lignes de financement :

1) Un financement est accordé pour l'achat d'équipements numériques sélectionnés (appareils, machines, systèmes et logiciels numériques, tels que des technologies de maison intelligente, 21 robots industriels, des imprimantes 3D et des supports d'enseignement et d'apprentissage numériques, tels que des tablettes et des écrans tactiles), afin de moderniser la formation des apprentis, en particulier pour ceux formés par les PME ;
2) Le programme finance également 8 projets pilotes dans des centres de compétences qui identifient les impacts de la numérisation sur les profils d'activité professionnelle et déterminent les exigences et les conséquences qui en découlent pour la qualification du personnel qualifié et du personnel de formation. Dans un deuxième temps, ils développent des concepts d'enseignement et d'apprentissage innovants pour la formation professionnelle 4.0 et les diffusent en tant que multiplicateurs. L'objectif est de faire en sorte que les résultats soient transférables et qu'il existe un large éventail d'applications.

Voici quelques exemples des projets pilotes susmentionnés :

● "Digital Media in VET" qui se terminera en 2022 et qui est composé de plusieurs sous-programmes avec différentes priorités de financement financent des projets nationaux de formation numérique qui développent de nouveaux scénarios d'apprentissage et des cours de formation initiale et continue modernes favorisant l'acquisition de compétences en matière de médias numériques ;

● " Qualification Initiative Digital Change - Q 4.0 ", qui, depuis 2018, finance le développement et l'expérimentation de concepts de formation complémentaire pour les formateurs de la formation professionnelle en entreprise. Le projet se compose de deux sous-projets : 1) séminaires MIKA (Media and IT Competence for Training Personnel) visant à promouvoir les compétences pédagogiques de base en matière de médias, le développement et le test de modules de formation continue pour renforcer les compétences de base en matière de médias et d'informatique du personnel de formation ; 2) Q 4.0 NETWORK visant à adapter le processus de formation au changement numérique, en tenant également compte des différences régionales et sectorielles. Dans les deux projets, le résultat final pourrait être un prototype d'offre de séminaire testé qui pourrait être mis à la disposition du personnel de l'EFP à l'échelle nationale ;

● "Digitalization II" depuis 2018 visant à identifier des stratégies pour concevoir des processus d'apprentissage qui utilisent le potentiel des médias numériques pour soutenir un apprentissage réussi, tant pour les individus que pour les groupes.

3.2 France - Internet Sans Crainte

(Étant donné le manque de bonnes pratiques dans le domaine de l'EFP dans ce pays spécifique, cette étude de cas a été sélectionnée en tant que pratique répondant aux contraintes requises mais ne concernant pas spécifiquement le secteur de l'EFP). Face aux cas constants de cyberintimidation, d'addiction à Internet, de rencontres dangereuses sur la toile, et à leurs conséquences tragiques pour de très jeunes élèves, il est devenu nécessaire d'attirer l'attention de tous sur les droits et les limites du comportement en ligne et, surtout, de présenter Internet comme un outil d'enrichissement et de divertissement exempt de danger. Créée en 2000, pionnière de la pédagogie numérique et experte en communication jeune public, Tralalere est une entreprise leader dans la production de programmes éducatifs cross-média : dessins animés pour productions multimédia, serious games, applications mobiles, eBooks, etc. Tralalere a notamment conçu et réalisé le programme national de sensibilisation aux risques sur Internet : www.internetsanscrainte.fr. Opéré par Tralalere depuis 2008, Internet Sans Crainte est le programme national pour aider les jeunes à mieux maîtriser leur vie numérique. Concrètement, Internet Sans Crainte propose une centaine de ressources gratuites et clés en main pour aider les enseignants, éducateurs et parents à accompagner les jeunes de 6 à 18 ans vers un usage éclairé et responsable des écrans et du numérique. Internet Sans Crainte propose également des conseils et une expertise pour accompagner les jeunes dans leur éducation numérique à travers des dossiers thématiques. Tralalere et Internet Sans Crainte coordonnent également Safer Internet France, programme national et européen pour la protection des mineurs sur Internet, aux côtés de la ligne Net Ecoute (e15 Enfance) et du Point de contact. A ce titre, Internet Sans Crainte organise en France le Safer Internet Day, une journée mondiale de sensibilisation des jeunes à un meilleur usage de l'Internet. Ce programme est soutenu par la Commission européenne dans le cadre du réseau Inhope/Insafe, qui regroupe 38 pays.

BÉNÉFICIAIRES

Internet Sans Crainte, propose tout au long de l'année des ressources numériques adaptées à différents publics,

notamment :

- Les médiateurs éducatifs (enseignants, animateurs, bibliothécaires, etc.) ;
- Les parents et les familles ;
- Les institutions et les associations.

3.3 Irlande - Cybersafe Kids

(Étant donné qu'un manque de bonnes pratiques dans le domaine de l'EFP existe dans ce pays spécifique, une pratique a été sélectionnée qui remplit les contraintes requises mais ne concerne pas spécifiquement le secteur de l'EFP).Cybersafe Kids en tant que projet a débuté en 2015 et est maintenant devenu une organisation caritative reconnue financée par un certain nombre de fonds philanthropiques irlandais tels que The Ireland Funds. Cybersafe Kids propose un certain nombre de programmes de formation axés sur la cybersécurité dans les écoles à travers le pays d'Irlande. La vision de Cybersafe Kids est celle d'un monde dans lequel les enfants utilisent la technologie de manière sûre, positive et réussie. Les principales parties prenantes de Cybersafe Kids sont les écoles participantes à travers l'Irlande (les élèves, les enseignants, les directeurs et les tuteurs), les universités de recherche partenaires, les bailleurs de fonds de l'organisation caritative et l'équipe impliquée dans l'exécution des programmes. L'objectif principal de l'organisation caritative est de faire progresser, de promouvoir et de fournir une éducation et une formation aux enfants, aux parents et aux enseignants de la communauté afin de garantir une navigation sûre et responsable dans le monde en ligne. En ce qui concerne l'impact, à ce jour, Cybersafe Kids a touché 24 000 enfants âgés de 8 à 13 ans via ses programmes scolaires. Rien qu'en 2020, les programmes ont permis de contacter 5 986 enfants et 1 554 parents dans 56 écoles en Irlande. En outre, une enquête en ligne anonyme a été distribuée et a permis de recueillir des données auprès de 3 764 enfants âgés de 8 à 12 ans concernant leur utilisation en ligne. Selon le rapport des directeurs (2019), les principaux domaines d'impact sont les suivants :

- L'exécution d'un programme d'éducation et le lancement d'un projet de mesure du changement de comportement en partenariat avec l'Université de Dublin et le Comité des enfants et des jeunes (CYPSC) ;

- L'accueil d'une forte campagne de la " Journée de la sécurité sur Internet " ;

● Lancement de contenus et de ressources en ligne ciblant les parents d'enfants plus jeunes (âgés de 2 à 10 ans). Les années précédentes, du matériel était publié pour les enfants plus âgés ;

● Élaboration d'une série de "demandes" politiques qui visent à avoir un impact sur la politique globale du pays.

3.4 Espagne – SPACE: Skills for school professionals against cyberbullying events

CONTEXTE.

La diffusion et l'utilisation généralisées des nouvelles technologies sont liées au phénomène de la cyberintimidation. En 2009, dans toute l'Europe, environ 18 % des jeunes européens âgés de 13 à 19 ans avaient été victimes d'intimidation/harcèlement/ harcèlement via l'internet et les téléphones mobiles, les taux actuels variant de 10 % à 52 %. Le Parlement européen souligne que la cyberintimidation a augmenté chez les enfants âgés de 11 à 16 ans, passant de 7 % en 2010 à 12 % en 2014.

LES BESOINS DES GROUPES CIBLES.

Le projet SPACE répond aux besoins de formation des enseignants des écoles, afin de leur faire acquérir des compétences pour prévenir/contraster la cyberintimidation. En effet, malgré le lancement par les États membres de l'UE de nombreuses initiatives et projets visant à prévenir et à combattre la cyberintimidation, celle-ci semble prendre de l'ampleur : comme il s'agit d'un phénomène nouveau, il manque un système organique de connaissances, de compétences et d'actions éducatives structurées garantissant que les enseignants acquièrent la connaissance de sa dynamique, la maîtrise des technologies numériques pour une utilisation sûre du Web, et les compétences pour planifier des actions de prévention, d'information et de formation.

OBJECTIFS.

De nombreuses ressources et contenus sur la cyberintimidation ont été développés par des écoles et des institutions ; néanmoins, il s'agissait d'initiatives isolées, non rassemblées dans un seul espace web et donc non valorisées. SPACE a relevé ce défi et a développé un MOOC - cours ouvert en ligne gratuit - sur la cyberintimidation pour les enseignants des écoles, ainsi qu'une bibliothèque numérique publique multilingue de ressources éducatives ouvertes sur la cyberintimidation. Principaux objectifs du projet :

- cartographier et décrire les compétences nécessaires pour prévenir et contrer la cyberintimidation ;
- développer une bibliothèque numérique de REL sur la cyberintimidation, avec des fonctions de recherche avancées ;
- de développer un MOOC pour les enseignants des écoles sur la cyberintimidation, en utilisant les REL précédemment récupérés et étiquetés ;
- potentialiser et améliorer chez les enseignants concernés la compétence numérique, à savoir la cybersécurité, le risque web et l'étiquette du net ;
- soutenir les enseignants acquérant les compétences pour intervenir en cas de cyberintimidation à l'école et pour planifier et réaliser des activités d'information et de formation avec leurs élèves.

PARTICIPANTS.

Le principal groupe cible impliqué dans le projet est représenté par les enseignants des écoles (niveaux CITE 2 et CITE 3). Les groupes cibles indirects sont les directeurs d'école et le personnel non enseignant, les étudiants, les parents, les autorités scolaires et les décideurs. 139 enseignants ont été impliqués dans l'essai du MOOC et 300 ont participé aux événements multiplicateurs organisés dans les pays partenaires. La bibliothèque numérique publique a reçu plus de 8 000 visites pendant le cycle de vie du projet.

ACTIVITÉS.

Le projet a duré 24 mois, au cours desquels les activités suivantes ont eu lieu :

● réalisation d'une carte des compétences et d'un modèle de MOOC ;

● conception et développement d'une bibliothèque numérique en ligne sur la cyberintimidation ;

● récupération, catalogage et identification des REL sur la cyberintimidation, et mise en œuvre de ces ressources dans la bibliothèque numérique ;

● la mise en place et la personnalisation d'une plateforme CMS pour héberger le MOOC ;

● conception, développement et test d'un MOOC multilingue sur la cyberintimidation ;

● création d'une boîte à outils contenant des indications, des lignes directrices et des recommandations sur le système et les outils SPACE ;

● réalisation de 10 événements multiplicateurs dans les pays partenaires et d'une conférence finale ;

● la réalisation de 4 réunions de consortium ;

● la diffusion par la création d'un site web, de brochures, de présentations, la participation en tant que reporter invité à la foire DIDACTA à Florence, des articles dans des magazines et des journaux.

IMPACT .

Le projet a produit un impact positif, favorisant la sensibilisation à la cyberintimidation, une meilleure connaissance de sa dynamique et des méthodes de prévention et de contraste, et développant un ensemble multidimensionnel de connaissances et de compétences dans le groupe d'enseignants européens impliqués. Les enseignants et les organisations impliqués dans le test ont acquis des compétences pour prévenir et contraster la cyberintimidation, des compétences numériques spécialisées sur la cybersécurité, les risques du web et l'étiquette du net, ont développé des compétences stratégiques et méthodologiques-didactiques améliorant leur professionnalisme pédagogique, disposent d'instruments plus efficaces pour mener à bien des activités d'information et de formation de leurs élèves pour prévenir la cyberintimidation.

3.5 Lettonie - Programme “Amélioration de la compétence numérique des enseignants sous la forme d'un environnement électronique pour l'utilisation des technologies éducatives".

OBJECTIF.

L'objectif du programme est d'améliorer la compétence numérique des éducateurs - enseigner les technologies et les outils qui aideront les éducateurs à organiser leur processus de travail plus efficacement. Le programme est mis en œuvre par depuis 2014 par le ministère de l'éducation et des sciences de la République de Lettonie.

BÉNÉFICIAIRES.

Le contenu des cours de 2020 est destiné à :

- les équipes de direction des établissements d'enseignement ;

● aux éducateurs des établissements d'enseignement professionnel (EFP) et d'enseignement général ;

● les enseignants des écoles primaires ;

● les enseignants des écoles maternelles ;

● les enseignants de diverses matières (mathématiques, langue lettone, informatique, ingénierie, conception et technologie, physique, chimie et biologie).

DESCRIPTION.

En 2020, le ministère de l'Éducation et des Sciences a fait de l'amélioration de la compétence numérique des éducateurs un objectif prioritaire de la compétence professionnelle, en allouant des fonds supplémentaires. Le programme offre des cours gratuits pour les éducateurs ayant différents niveaux de connaissances et représentant divers sujets (leur domaine de spécialisation, voir la section Bénéficiaires). Les responsables de la mise en œuvre des cours ont élaboré des tâches d'apprentissage détaillées, ont attiré des chefs de groupe - des consultants pour assurer un régime d'apprentissage favorable pour les éducateurs. Le contenu des cours est conçu en fonction des exigences de l'environnement d'apprentissage moderne.

RÉSULTATS OBTENUS.

4339 éducateurs ont suivi des cours de développement des compétences professionnelles longs (avec le droit accordé de travailler en tant qu'enseignant en informatique) et courts (2014).

et courts cours de développement des compétences professionnelles (2014-2020).

INNOVATION.

L'approche innovante fait obstacle à l'organisation du processus - chaque participant au cours peut apprendre le contenu à un rythme et à un moment qui lui conviennent.

contenu à un rythme et à un moment qui lui conviennent. Pendant le cours, on analyse les technologies et les outils qui peuvent être utilisés dans le processus d'étude afin de promouvoir la collaboration et de simplifier l'organisation du processus d'étude/de travail des éducateurs.

3.6 Portugal

Malgré quelques initiatives ad hoc, les actions de formation dans le domaine de la cybersécurité pour l'EFP n'ont pas été identifiées. Seuls quelques cours d'enseignement supérieur, de troisième cycle ou de nature commerciale ont été identifiés sur le marché. La formation à la cybersécurité pour l'EFP devrait donc être une priorité fondamentale pour étayer l'avenir plus sûr de notre pays, à savoir capable de garantir la sécurité des personnes et des entreprises.

Le Centre National de Cybersécurité, avec la mission de promouvoir le partage des connaissances et une culture nationale de la Cybersécurité, a développé le Programme de Sensibilisation et de Formation en Cybersécurité, à travers lequel il est prévu de massifier la formation et la sensibilisation des citoyens et des employés des organisations aux dangers de l'utilisation non informée du cyberespace, en réalisant des actions de sensibilisation et de formation en Cybersécurité dans différentes parties du pays, du nord au sud, en passant par les îles, avec le soutien de partenaires, mais rien de dirigé vers les Institutions de Formation Professionnelle.

3.7 Italy - Docenti connessi e sicuri (Des enseignants connectés et en sécurité)

CONTEXTE.

Le programme a pour objectif général de mener des actions visant à innover et à renforcer les compétences numériques dans les écoles. Plus précisément, le programme vise à améliorer les compétences et les connaissances des enseignants concernant les nouvelles expériences d'enseignement numérique intégré, le fonctionnement et les avantages de l'Internet des objets et l'importance de la cybersécurité. Le programme est promu dans le cadre du nouveau protocole d'accord entre le ministère de l'Éducation (Italie) et Cisco.

GROUPES CIBLES.

Les bénéficiaires du programme sont les enseignants des écoles italiennes de tout ordre et de toute classe.

ACTIVITÉS.

Le programme de formation proposé par Cisco aux enseignants consiste en 3 webinaires auxquels sont liés 3 cours approfondis. La participation à l'ensemble du programme est totalement gratuite.

1. Un monde numérique connecté Webinaire "DAD et nouvelles expériences d'enseignement numérique intégré" organisé par le personnel de Cisco ou les partenaires de Cisco et cours en ligne lié "Get Connected". Durée estimée de la formation : 30 heures Présentation du cours : Le cours vous apprend à développer des connaissances numériques de base. La structure particulièrement interactive du cours crée un environnement facilement accessible pour un public abordant le monde de l'informatique pour la première fois.

2. Des citoyens numériques conscients : Webinaire "Smart City et Internet des objets : nouveaux services numériques pour les citoyens" organisé par le personnel de Cisco ou les partenaires de Cisco et cours en ligne lié "Introduction à l'Internet des objets (IoT)". Durée estimée de la formation : 20 heures Aperçu du cours : Le cours Introduction à l'IoT (Internet des objets) présente aux enseignants les technologies qui prennent en charge l'IoT et les opportunités générées par le nombre croissant de connexions réseau entre les personnes, les processus, les données et les objets.

3. Sécurité informatique : Webinaire "Comment se protéger des menaces du réseau" organisé par le personnel de Cisco ou les partenaires de Cisco et cours en ligne lié "Introduction à la cybersécurité". Durée estimée de la formation : 20 heures. Aperçu du cours : Le cours Introduction à la cybersécurité analyse les tendances du monde informatique, les menaces et le fait d'être en totale sécurité dans le cyberespace, en protégeant ses données personnelles.

IMPACT.

Le projet s'étant terminé le 3 juin, les chiffres concernant les enseignants formés sont encore en cours d'élaboration. Cependant, le projet est innovant car il combine une formation technologique avec l'entrepreneuriat numérique, mais aussi avec la programmation.

Conclusion

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 ce sujet émergent dans tous les États membres.

Néanmoins, les initiatives existantes sont complètes et se sont avérées efficaces (voir la section Bonnes pratiques). 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 niveau 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 au cyberharcèlement 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 toute utilisation.

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.

Références

ADEI (2017), El trabajo del futuro. Technical Note.

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

Andries B. et Beigbeder I. (coordonné par) (1993), La culture scientifique et technique pour les professeurs des écoles, Paris: Hachette éducation, CNDP.

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

Baron G.-L. et Bruillard É. (2000), Technologies de l'information et de la communication dans l'éducation : Quelles compétences pour les enseignants?, Éducation et Formation, No 56.

Baron G.-L. et Bruillard É. (sous la direction) (2002), Les technologies en éducation: perspectives de recherche et questions vives, Actes du Symposium international francophone, Paris : INRP, IUFM de Basse-Normandie, MSH.

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

Blanco, R., Fontrodona, J., Poveda, C. (2017), La industria 4.0: el estado de la cuestión, Revista Economía Industrial, No 406.

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.

Capelle, C., Cordier, A., Lehmans, A., (2018), Usages numériques en éducation : l'influence de la perception des risques par les enseignants, Open Edition Journals.

Carrizosa Prieto, E (2018), Lifelong learning e industria 4.0. Elementos y requisitos para optimizar el aprendizaje en red., Revista internacional y comparada de relaciones laborales y derecho del empleo. Vol. 6, No 1.

Central Statistics Office (CSO) (2018), Information Society Statistics – Households: https://www.cso.ie/en/releasesandpublicatons/er/isshh/informationsocietystatisticshouseholds2018/ (accessed on 6th July, 2021).

CEFEDOP, (2021), Vocational education and training in Portugal, EU Agenda.

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).

Database of National Education Opportunities – Niid.lv, study programmes in cybersecurity

Department of Education and Skills, Government of Ireland (2015), Digital Strategy for Schools (2015-2020)-Enhancing Teaching, Learning and Assessment.

Department of Education and Skills, Government of Ireland (2017), Higher Education System Performance Framework 2018-2020.

Department of Enterprise, Trade and Employment (2018), Future Jobs Ireland – Preparing Now for Tomorrow's Economy.

Department of Further and Higher Education, Research, Innovation and Science, Government of Ireland (2021), Statement of Strategy 2021-2023.

Department of Justice (2021). Cybercrime: www.justice.ie/en/jelr/pages/cybercrime (accessed on 2nd July, 2021).

Department of Tourism, Culture, Arts, Gaeltach, Sport and Media (2019), Action Plan for Online Safety 2018 – 2019.

Dig8tal (2020), Is German Cybersecurity ready for 2021?, https://dig8ital.com/resources/library/is-german-cyber-security-ready-for-2021

Erasmus+ project DIG4VET (Digital Tools for Learning and Validation in VET and WBL: Training Program
for VET Teachers, Trainers and Potential I-Coaches)

Escuela de organizacion industrial, Activa industria 4.0.

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

European Commission (2020), Italy in the Digital Economy and Society Index.

European Commission (2020), Lettonie in the Digital Economy and Society Index.

Federal Office For Information Security, (2019),The State of IT Security in Germany in 2019.

Federal Office For Information Security, (2020), The State of IT Security in Germany in 2020.

Federal Office For Information Security, (2020). Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit.

Government of Ireland (2018), National Cyber Security Strategy 2019-2024.

Government of Italy (2020), Piano Nazionale di Ripresa e Resilienza -PNRR.

Government of Lettonie, (2019), Informative report, Cybersecurity Strategy of Lettonie.

Government of Lettonie, (2020), Education Development Guidelines 2021-2027 "Future Skills for the Future Society".

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

Guir R. (2002), Pratiquer les TICE : Former les enseignants et les formateurs à de nouveaux usages, Bruxelles: De Boeck et Larcier.

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.

Joseph, V. (2020). Vocational education and training for the future of work: France, Cedefop ReferNet thematic perspectives series.

Kultusministerkonferenz (2016), "Bildung in der digitalen Welt: Strategie der Kultusministerkonferenz"

Lardellier P., Moatti, D. (2014), Les ados pris dans la Toile. Des cyberaddictions aux techno-dépendances, Paris: Éditions Le Manuscrit, Coll. « Addictions : Plaisir, Passion, Possession »

Lettonien Safer Internet Centre (Project-platform "Drossinternets.lv"): https://drossinternets.lv/

LIKTA (Lettonien Information and Communication Technologies Association): https://likta.lv/digitalasparmainas-izglitiba/

Likumi.lv, Noteikumi par pedagogiem nepieciešamo izglītību un profesionālo kvalifikāciju un pedagogu profesionālās kompetences pilnveides kārtību. https://likumi.lv/ta/id/301572-noteikumi-par-pedagogiem-nepieciesamo-izglitibu-un-profesionalo-kvalifikaciju-un-pedagogu-profesionalas-kompetences-pilnveides

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

Ministry of Education, University and Research, Government of Italy, Piano Nazionale Scuola Digitale – PNSD.

Ministry of Education, University and Research, Government of Italy, (2018), La Buona Scuola (Law No. 107/2015)

Ministry of Education, University and Research, Government of Italy (2020), Accordo di collaborazione per lo svolgimento di attività didattiche e formative congiunte per promuovere l'educazione alla cittadinanza digitale e l'utilizzo consapevole delle tecnologie digitali e dei social media, Memorandum of Understanding n. 4 of 28 October 2020.

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 Industry, Trade and Tourism, Government of Spain, Industria Conectada 4.0, Agenda Digital para Espana.

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

Mokhtar Ben Henda (2016), Identification des besoins en formation tic/e dans les pays francophones du sud. Étude réalisée par: Initiatives pour le Développement numérique de l'espace universitaire francophone francophone, [Rapport de recherche] Agence universitaire de la Francophonie.

National Centre for Vocational Education Research, (2020), Teaching digital skills: Implications for VET educators - good practice guide.

OECD (2021), Going Digital in Lettonie

OECD, (2018), TALIS - The OECD Teaching and Learning International Survey TALIS - OECD Teaching and Learning International Survey

Pridzans, Dzerviniks (2019), The Topicality of Educators' Digital Competence Development, SOCIETY. INTEGRATION. EDUCATION Proceedings of the International Scientific Conference. Volume V, May 24th -25th.

Principes et organisation de la deuxième année de la formation des enseignants stagiaires en IUFM, (2002). La circulaire du 4 avril 2002 parue au Bulletin officiel n° 15 du 11 avril 2002.

Saldus Technical School, Study Programme Civil Security and Defence: https://www.saldustehnikums.lv/izglitibas-iespejas/profesijas/profesionala-videja

Stolterman, E (2004), Information Technology and the Good Life, International Federation for Information Processing Digital Library; Information Systems Research. Volume 143.

Télé-enseignement : les 5 risques majeurs en matière de cybersécurité – Sophos News

Thélot C. (sous la direction) (2004), Pour la réussite de tous les élèves, rapport officiel de la Commission du débat national sur l'avenir de l'École, Paris : La documentation Française.

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 :