ESSACHESS – Journal for Communication Studies

Stratégies discursives numériques dans la lutte officielle contre la cybercriminalité au Nord et au Sud. Analyse lexicométrique de deux sites web marocain et français

ESSACHESS –
Journal for Communication Studies
Volume 17 Issue 2(34), p. 51-71
© The Author(s) 2024
Reprints and Permission:
© ESSACHESS
https://www.essachess.com/
DOI: 10.21409/essachess.1775-352x

Cite : CHAKOUK, S. (2024). Stratégies discursives numériques dans la lutte officielle contre la cybercriminalité au Nord et au Sud. Analyse lexicométrique de deux sites web marocain et français. *ESSACHESS*. 17(34): 51-71. https://doi.org/10.21409/XVRW-A145

Said CHAKOUK
Maître de Conférences HDR, Université Mohammed V de Rabat, MAROC
e-mail: s.chakouk@um5r.ac.ma

Résumé : La cybercriminalité est un domaine de recherche qui se distingue par la multitude de méthodologies utilisées, allant de l'approche anthropologique à la psychanalytique, en passant par la sociologique, le droit et la communication. Dans le champ des sciences de l'information et de la communication (SIC), les recherches se sont centrées plutôt sur les dispositifs techniques et juridiques. Notre contribution vise à explorer comment les médias émergents contribuent à lutter contre la cybercriminalité au prisme d'une analyse lexicométrique des plateformes de cybersécurité officielles, en utilisant le « web scraping », une technique de Big Data dédiée à l'extraction des données volumineuses. L'analyse lexicométrique de deux

Article received on September 11, 2023. Article accepted on September 18, 2024.
Conflict of Interest: The author(s) declare(s) no conflict of interest.

sites web officiels montre des approches distinctes et complémentaires focalisées sur la sensibilisation, la lutte contre la désinformation et la protection des enfants en ligne, d'une part, et la sécurité des données personnelles et financières ainsi que les aspects juridiques et répressifs de la cybercriminalité, d'autre part. Ces différences reflètent les spécificités culturelles et légales des contextes Nord-Sud, tout en enrichissant la compréhension des stratégies de prévention numérique.

Mots-clés : médias numériques, cybercriminalité, lexicométrie, Big Data, stratégies

***

Discursive Strategies on the Internet in the Official Fight Against Cybercrime in Morocco and France: A Lexicometric Analysis of Moroccan and French Websites

Abstract : Cybercrime is a field of research that is distinguished by the multitude of methodologies used, ranging from the anthropological to the psychoanalytic, through sociology, law and communication. In the field of information and communication sciences (ICS), research has focused rather on technical and legal devices. Our contribution aims to explore how emerging media contribute to combating cybercrime through the prism of a lexicometric analysis of official cybersecurity platforms, using "web scraping", a Big Data technique dedicated to the extraction of large data. The lexicometric analysis of two official websites shows distinct yet complementary approaches. One focuses on raising awareness, combating disinformation, and protecting children online, while the other emphasizes the security of personal and financial data as well as the legal and punitive aspects of cybercrime. These differences reflect the cultural and legal specificities of the North-South contexts while enhancing the understanding of digital prevention strategies.

Keywords : digital media, cybercrime, lexicometry, media discourse, Big Data, strategies

***

Introduction

Dans le domaine des Sciences de l'Information et de la Communication (SIC), les études se sont principalement concentrées sur les aspects techniques (Cardiet & De Vectra, 2023 ; Pertus, 2023 ; Ndemo, 2023) et juridiques (Pereira, 2016 ; Gillwald, 2022 ; Haounani, 2023 ; Bellon, 2023 ; Chirwa & Ncube, 2023). Ces recherches ont permis de cerner les défis liés à la régulation des données personnelles, la propriété intellectuelle et la sécurisation des échanges en ligne. Par exemple, Cardiet et De Vectra (2023) explorent les implications des nouvelles technologies sur la protection de la vie privée, tandis que Gillwald (2022) examine le cadre juridique nécessaire pour faire face à la cybercriminalité dans un contexte globalisé.

Dans ce contexte, il est également important de considérer comment l'usage des médias numériques impacte la mobilisation sociale. Les travaux sur l'usage des médias numériques ont démontré leur rôle clé dans la mobilisation sociale, comme le

montre le Printemps arabe et les Gilets jaunes (Daghmi et al., 2012 ; 2013; Proulx, 2020). Ces événements soulignent l'importance d'une éducation numérique et d'une sensibilisation aux risques associés, notamment la désinformation et la cybercriminalité. Bien que ces plateformes offrent des opportunités d'engagement, elles posent aussi des défis qui rendent nécessaires des stratégies de prévention pour protéger les utilisateurs en ligne.

Ainsi, la cybercriminalité s'inscrit dans la dynamique des soulèvements populaires par différents aspects (Menusier, 2021). Tout d'abord, elle exploite les mêmes outils technologiques utilisés pour mobiliser les masses pendant ces soulèvements. Les plateformes de médias sociaux et les applications de messagerie instantanée, catalyseurs majeurs des mouvements populaires, sont utilisées par les cybercriminels pour coordonner leurs activités et cibler leurs victimes (Ghernaouti, 2023). Ensuite, la médiatisation des soulèvements populaires a non seulement augmenté la visibilité des problèmes sociaux et politiques, mais a également mis en lumière les vulnérabilités des infrastructures numériques (Granjon, 2018 ; Brotcorne, 2010) . Ces failles sont fréquemment exploitées par les cybercriminels pour mener des attaques informatiques, compromettant ainsi la sécurité des individus et des institutions.

Dans cette perspective, notre étude vise à analyser comment les médias numériques peuvent être mobilisés dans la lutte contre la cybercriminalité. Bien que les cybercriminels utilisent ces plateformes, elles offrent également un terrain que les autorités de sécurité en ligne peuvent utiliser pour contrer leurs activités. La lutte contre la cybercriminalité, une préoccupation majeure à l'échelle mondiale, a engendré un besoin de sensibilisation accrue des utilisateurs aux pratiques sécurisées en ligne. Dans ce cadre, les sites web officiels des gouvernements et des organismes de sécurité sont devenus indispensables. Nous nous sommes penchés sur l'analyse de ces sites afin de décéler en quoi ces plateformes officielles s'avèrent efficaces.

1. Analyse discursive de la cybercriminalité : une approche enrichie par la lexicométrie

1.1. *Cybercriminalité : un concept confus*

Malgré les nombreuses tentatives visant à fournir une définition et une classification plus appropriées de la cybercriminalité, à la fois dans un contexte théorique et pratique, grâce aux travaux de chercheurs comme Brenner et Koops (2004), Phillips (2006), Leman-Langlois (2006) et Jewkes et Yar (2010), il n'existe toujours pas de consensus universel à cet égard. Dans ce sens, Décary-Hétu (2020) souligne que la cybercriminalité, terme journalistique sans définition légale dans la plupart des pays, reste floue. Les traités internationaux évitent également une définition précise, optant pour des approches fonctionnelles. Actuellement, des débats aux Nations Unies concernant une nouvelle convention sur la cybercriminalité risquent de fragiliser celle

de Budapest[1]. Même cette dernière n'a pas réussi à fournir une définition claire du concept de « cybercriminalité ».

Les définitions du terme cybercriminalité viennent donc du monde scientifique avec des interprétations variées. Schell & Martin (2004), cités par Décary-Hétu (2020), décrivent la cybercriminalité en lien avec la technologie, tandis que Wall (2007), cité par Kirsty et al. (2022), la restreint aux activités nuisibles pour un gain personnel. Actuellement, l'accent est mis sur les définitions englobant les crimes facilités par la technologie. Gordon & Ford (2006) préconisent celle-ci pour sa simplicité, Chawki (2006), Conseiller d'État adjoint et président de l'AILCC[2], la présente comme étant toute activité illégale liée à l'interconnexion de systèmes informatiques et de réseaux de télécommunication, dont la réalisation serait impossible sans cette interconnexion. En effet, selon Pereira (2016), les termes « cybersécurité », « cyberdéfense » et « cybercriminalité » sont souvent utilisés de manière interchangeable sans qu'il existe des définitions précises établies par le droit. Cette confusion dans l'utilisation des termes peut compliquer la compréhension et la réglementation de ces concepts liés à l'environnement numérique et à la criminalité en ligne.

Dans cet article, nous adoptons la définition du Sénat en France [3] : « La cybercriminalité – les juristes préfèrent le terme de cyberdélinquance – recouvre une réalité protéiforme et mal cernée. Il n'existe en effet aucune définition conventionnelle ou légale unanimement admise de la cybercriminalité. Celle-ci peut se concevoir comme toute action illégale dont l'objet est de perpétrer des infractions pénales sur ou au moyen d'un système informatique interconnecté à un réseau de télécommunications ».

1.2. *Analyse discursive et la cybercriminalité*

Les chercheurs en SIC reconnaissent que l'approche communicationnelle est déterminante dans la prévention de la cybercriminalité (Wall, 2024 ; Pereira, 2016 ; Bougren & Chadi, 2023). Pour Moussaoui (2017), la communication permet de sensibiliser le public aux risques de la cybercriminalité et de promouvoir des comportements sécurisés en ligne. L'approche communicationnelle permet de comprendre comment les messages sont construits, diffusés et interprétés dans le contexte de la cybercriminalité.

Dans ce contexte, l'analyse discursive facilite la compréhension des messages et discours liés à la cybercriminalité. Selon Fairclough (2003), cette analyse permet

---

[1] Cf. Convention-Cadre de la cybercriminalité adoptée en 2001 à l'échelle internationale.

[2] Cf. Association Internationale de Lutte Contre la Cybercriminalité (AILCC).

[3] Cf. Joissains, S., & Bigot, J. (2020). Rapport d'information sur la lutte contre la cybercriminalité (N° 613). Sénat, session extraordinaire de 2019-2020. Commission des affaires européennes et Commission des lois. Enregistré à la Présidence du Sénat le 9 juillet 2020.

d'explorer les pratiques langagières et discursives utilisées dans la communication sur la cybercriminalité, en mettant en évidence les représentations, les significations et les rapports de pouvoir véhiculés. En utilisant cette approche, il devient possible d'analyser les stratégies discursives utilisées pour prévenir et lutter contre la cybercriminalité.

En s'appuyant sur les recherches de De Bruijn et Janssen (2017), on note que les stratégies discursives contribuent à la transmission des informations claires et persuasives aux utilisateurs, favorisant ainsi l'adoption de comportements sécurisés en ligne. En effet, les discours employés dans la sensibilisation à la cybercriminalité doivent être bien construits et adaptés au public cible afin de maximiser leur impact. Khelifi (2016) a étayé cette idée en se focalisant sur l'analyse lexicométrique en tant qu'approche qui vise l'étude des stratégies discursives, permettant de quantifier les occurrences des mots-clés pertinents et d'identifier les schémas récurrents présents dans les discours. Cette méthode nous aide à mieux comprendre comment les messages sont construits et comment ils peuvent influencer les attitudes et les comportements des utilisateurs. De plus, les travaux de Bisiania (2020) montrent que l'aspect dynamique de l'analyse lexicométrique permet d'analyser les évolutions des stratégies discursives dans la détection et la prévention de la cybercriminalité, en examinant les variations discursives entre différentes campagnes de prévention. Cette approche permet de mesurer l'efficacité des messages et d'adapter les terminologies utilisées en fonction des nouveaux défis des politiques sécuritaires européennes, y compris la cybercriminalité.

A cet effet, Wybo et al. (2015) mettent en évidence l'importance des messages d'alerte pour prévenir la cybercriminalité, en sensibilisant les utilisateurs aux risques en ligne et en les incitant à prendre des mesures de sécurité. Les témoignages personnels créent une connexion émotionnelle en partageant des expériences réelles de victimes ou d'experts en cybersécurité. Perwej et al. (2021) soulignent à ce niveau que les statistiques, telles que le nombre d'attaques signalées ou les pertes financières causées par la cybercriminalité, servent de preuves tangibles pour encourager les utilisateurs à adopter des comportements sécurisés.

1.3. *La médiatisation dans l'analyse discursive de la cybercriminalité*

Dans notre analyse discursive de la cybercriminalité, nous considérons la médiatisation comme approche théorique qui explique la construction sociocommunicative de nos sociétés et des domaines de la réalité. Nous nous appuyons sur les recherches de Tudor et Bratosin (2020), qui explorent l'impact de la médiatisation et des enjeux technologiques sur notre vision de l'avenir, mettant en lumière la diversité des discours et des perspectives. Ces travaux fournissent une base pour explorer les différentes visions technologiques, du pessimisme à l'optimisme, et soulignent l'importance de comprendre ces perspectives dans un monde en constante évolution. Dans notre étude, nous nous appuyons sur l'importance des médias émergents dans la diffusion d'informations sur la cybercriminalité, influençant ainsi les représentations sociales et les attitudes du public envers ce phénomène.

Dans ce cadre, les stratégies discursives constituent des leviers importants dans la prévention de la cybercriminalité. L'analyse lexicométrique nous permet de contribuer aux recherches qui étayent cette thèse et d'approfondir la compréhension des stratégies de lutte à partir des données quantitatives et sur la base de l'identification des schémas discursifs récurrents et de la détection des évolutions des messages de prévention. Cette approche nous fournit des informations précieuses pour améliorer l'efficacité des campagnes de sensibilisation qui visent l'établissement d'espaces en ligne plus sécurisés. Notre objectif n'est pas seulement d'examiner les stratégies et politiques visant à prévenir la cybercriminalité en tant qu'acte criminel, mais aussi de décrypter la manière dont le terme est utilisé en relation avec son contexte discursif.

2. Précisions méthodologiques

2.1. *Lexicométrie : Étude statistique de l'usage des mots comme outil quantitatif pour des analyses qualitatives*

Selon Leblanc (2011), la lexicométrie a émergé en France, dans les années 70 sous le nom de statistique linguistique (Guiraud, 1960), de statistique lexicale (Muller, 1964) et l'analyse statistique des données textuelles (Benzécri et al., 1973 ; Benzécri, 1980; 1982). Avec le temps, différentes approches telles que la textométrie, la logométrie et l'analyse de discours assistée par ordinateur sont apparues pour refléter les nuances du domaine. La transition de la lexicométrie à la textométrie s'est faite en prenant en compte des unités textuelles plus larges, comme les zones, les paragraphes et les segments textuels, permettant d'explorer de nouveaux phénomènes cooccurrentiels du texte.

Pour notre étude, nous adoptons la définition de Poudat et Landragin (2017) selon laquelle la lexicométrie consiste en l'étude statistique de l'usage des mots. Nous considérons l'analyse lexicométrique comme un outil quantitatif permettant d'identifier des indices servant de symptômes (Charaudeau, 2009). Ensuite, nous réaliserons des analyses qualitatives basées sur des hypothèses. Ainsi, nous abordons la lexicométrie en utilisant des méthodes statistiques pour quantifier les relations lexicales, identifier les schémas discursifs récurrents et mettre en évidence les associations sémantiques dans un corpus**.**

2.2. *Corpus d'étude*

Nous avons sélectionné deux sites web pour notre étude : www.e-himaya.gov.ma et www.cybermalveillance.gouv.fr. Leur sélection repose sur leur pertinence dans le domaine de la prévention de la cybercriminalité et sur l'accessibilité et la disponibilité de leurs contenus en ligne.

La méthodologie adoptée repose sur une approche comparative mixte, combinant des éléments quantitatifs et qualitatifs dans les discours des deux sites. Nous avons utilisé des techniques d'analyse lexicométrique pour examiner les caractéristiques

linguistiques des discours présents sur les deux sites web. Cette analyse nous permettra d'identifier les mots clés, les thèmes récurrents et les schémas discursifs utilisés pour aborder la cybercriminalité.

Dans un premier temps, nous avons effectué la collecte des données en explorant les pages de deux sites web choisis. Pour cela, nous avons utilisé une méthode de big data connue sous le nom de « web scraping » par le logiciel « Octoparse »[4], qui nous a permis d'extraire les informations des sites web.

- Plateforme https://www.e-himaya.gov.ma/: notre étude s'est concentrée exclusivement sur les contenus présents dans la rubrique *Initiatives*. Ce sont des initiatives menées par les acteurs marocains chargés de la protection en ligne ainsi que les guides et les conseils (Figure 1).

Figure 1. *Plateforme https://www.e-himaya.gov.ma/*

- Plateforme https://www.cybermalveillance.gouv.fr/cybermenaces/:Nous avons restreint notre analyse aux seuls contenus des rubriques « Les Menaces et Bonnes Pratiques : Particulier » (Figure 2).

[4] https://www.octoparse.fr/.

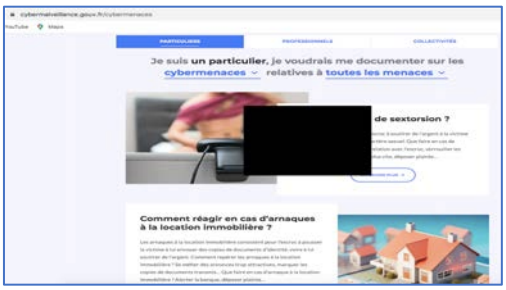

Figure 2. *La plateforme https://www.cybermalveillance.gouv.fr/cybermenaces/*

Nous avons effectué une analyse lexicométrique à l'aide du logiciel IramuteQ[5]. C'est un logiciel libre conçu pour l'analyse de données textuelles en sciences humaines et sociales, qui s'appuie sur le langage de programmation R pour le traitement statistique. Il permet de traiter et d'explorer des corpus variés et volumineux grâce à des outils d'analyse qualitative tels que l'analyse lexicale et la création de nuages de mots. Iramuteq facilite l'identification de thèmes et de tendances dans les données textuelles, rendant l'analyse plus accessible et intuitive.

3. Résultats et discussion

L'analyse lexicométrique de ces deux sites web par Iramuteq a révélé plusieurs éléments clés sur les stratégies discursives employées pour la prévention de la cybercriminalité.

3.1. *Nuages de mots*

3.1.1. Présentation des résultats obtenus

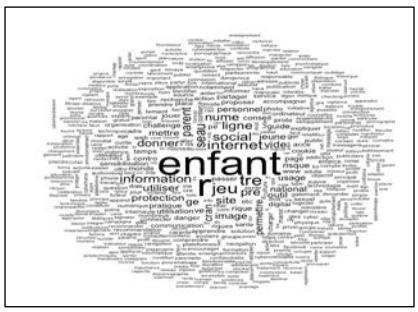

Figure 3. *Nuage de mots d'E-himaya*

Figure 4. *Nuage de mots de* cybermalveillance

[5]Plus de details ici; http://www.iramuteq.org/

Dans ce qui suit, nous présentons l'analyse des termes les plus récurrents dans les deux nuages de mots respectifs des deux contenus, Cybermalveillance et E-himaya.

Pour le contenu du E-himaya (Figure 3), les termes prédominants sont centrés autour de la culture digitale et de la prévention de la cybercriminalité. On retrouve des termes tels que « information », « enfant », « fakenews », « faux », « en ligne », « social », « réseaux », « internet », « utiliser » et « donner ». Ces termes soulignent l'importance de l'information, de la sensibilisation, de la prévention des fausses informations et de la promotion d'une utilisation responsable et sécurisée d'Internet, en particulier dans le cadre d'une approche éducative.

Quant au contenu du Cybermalveillance (Figure 4), les termes prédominants sont liés à la prévention de la cybercriminalité : « Victime », « Donnée », « Compte », « Bancaire », « Message », « Service », « Amende », « Emprisonnement » et « Frauduleux ». Ces termes mettent l'accent sur la protection des données personnelles et financières, ainsi que sur les aspects juridiques et répressifs liés aux activités criminelles en ligne.

3.1.2. Analyse et interprétation des résultats

En comparant les contenus des deux sites, nous constatons que, bien qu'ils se focalisent sur la prévention de la cybercriminalité, ils privilégient des aspects différents. Le contenu E-himaya valorise l'éducation digitale, la sensibilisation et la prévention des risques liés à l'utilisation d'Internet, en soulignant des thématiques spécifiques telles que les fausses informations et la protection des enfants en ligne, sans oublier l'importance de développer une culture numérique responsable, tandis que le contenu de Cybermalveillance se concentre davantage sur la protection des données personnelles et financières, ainsi que sur les aspects juridiques et répressifs.

3.2. *Classification descendante hiérarchique (CDH)*

3.2.1. Présentation des résultats obtenus

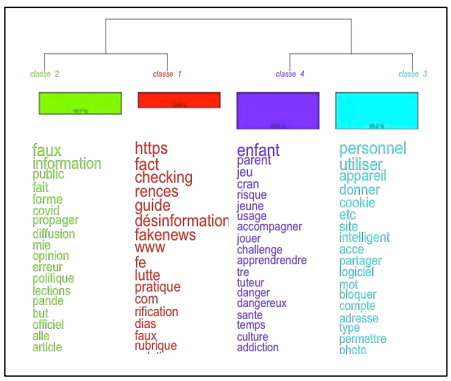

Figure 5. *Classification descendante hiérarchique (CDH) E-himaya*

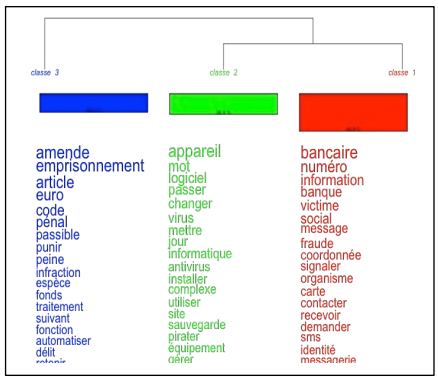

Figure 6. *Classification descendante hiérarchique (CDH)* Cybermalveillance

Le dendrogramme d'E-Himaya (Figure 5) révèle deux branches distinctes :

- *Branche 1* qui regroupe les classes 1 et 2. La classe 1 (13,9%) est caractérisée par des termes tels que « fact », « checking », « guide », « désinformation », « fackenews », « site », « lutte », « pratique », « vérification », « faux » et « rubrique ». Ces termes sont liés à la vérification des faits et à la lutte contre la désinformation. La classe 2 (19,7%) est caractérisée par des termes tels que « faux », « information », « public », « fait », « fake news », « forme », « covid », « propager », « diffusion », « opinion », « erreur », « politique », « but », « officiel » et « article ». Ces termes sont également liés à la vérification des faits et à la diffusion d'informations fiables. Ainsi, la branche 1 se concentre sur la dimension de la vérification des faits et de la lutte contre la désinformation.

- *Branche 2* qui regroupe les classes 3 et 4. La classe 3 (33,2%) est caractérisée par des termes tels que « enfant », « parent », « jeu », « risque », « jeune », « usage », « accompagner », « jouer », « challenge », « apprendre », « tuteur », « danger », « dangereux », « santé », « temps », « culture » et « addiction ». Ces termes sont liés à la sensibilisation et à la protection des enfants en ligne, ainsi qu'à la gestion du temps passé sur les jeux et les médias numériques. La classe 4 (33,2%) est caractérisée par des termes tels que « personnel », « utiliser », « appareil », « donner », « cookie », « site », « intelligent », « accès », « partager », « logiciel », « mot », « bloquer », « compte », « adresse », « type », « permettre » et « photo ». Ces termes renvoient aux aspects liés à l'utilisation personnelle des appareils numériques, à la protection des données personnelles et à la sécurité en ligne.

Nous constatons que la branche 1 se concentre sur la vérification des faits et la lutte contre la désinformation, tandis que la branche 2 aborde les aspects de sensibilisation et de protection des enfants en ligne, ainsi que l'utilisation personnelle des appareils numériques et la sécurité des données. Cette distinction entre les deux branches permet de mettre en évidence les différentes dimensions de la prévention de la cybercriminalité abordées par le site E-Himaya.

Le dendrogramme Cybermalveillance (Figure 6) met en avant les données suivantes :

- *Branche 1* : la classe 1 (48,8%) est axée sur la protection des données personnelles et la prévention des fraudes en ligne. Les termes associés à cette classe, tels que « bancaire », « numéro », « information », « banque », « victime », « social », « message », « fraude », « coordonnée », « carte », « contacter », « recevoir », « demande », « sms », « identité » et « messagerie », reflètent la préoccupation pour la sécurité des informations personnelles et la prévention des activités frauduleuses. La classe 2 (26,9%) de Cybermalveillance se concentre sur la sécurité des systèmes informatiques et la gestion des outils numériques. Les termes associés à cette classe mettent l'accent sur la protection contre les attaques informatiques, la gestion des logiciels et des équipements, ainsi que la sécurité des systèmes. On retrouve des termes tels que « appareil », « mots », « logiciel », « passer », « changer », « virus », « mettre à jour », « informatique », « antivirus », « installer », « complexe », « utiliser », « site », « sauvegarder », « pirater » et « équipement ».

- *Branche 2* : la classe 3 (24,2%) aborde les aspects juridiques et répressifs liés à la cybercriminalité. Les termes associés à cette classe tels que « amende, « emprisonnement », « article », « euro », « code », « pénal », « passible », « punir », « peine », « infraction », « espèce », « fonds », « traitement », « suivant », « fonction », « automatiser » et « délit », mettent l'accent sur les sanctions, les lois et les mécanismes juridiques impliqués dans la prévention et la répression des activités criminelles en ligne.

3.2.2. Analyse et interprétation des résultats

En comparant les deux cas, nous constatons que les contenus d'E-Himaya et de Cybermalveillance abordent tous les deux la prévention de la cybercriminalité, mais avec des emphases différentes, en couvrant d'autres aspects importants de la prévention de la cybercriminalité.

E-Himaya se concentre sur la sensibilisation, la vérification des faits et la lutte contre la désinformation. La branche 1 de son dendrogramme se concentre sur la vérification des faits, avec des termes liés à la lutte contre la désinformation tels que « fact checking », « désinformation », « fanews » et « vérification ». La branche 2 se focalise sur la sensibilisation et la protection des enfants en ligne, ainsi que sur l'utilisation personnelle des appareils numériques et la sécurité des données. En revanche, Cybermalveillance se concentre davantage sur la protection des données personnelles et financières, ainsi que sur les aspects juridiques et répressifs de la cybercriminalité. Son dendrogramme révèle trois classes distinctes : la protection des données personnelles et la prévention des fraudes en ligne, la sécurité des systèmes informatiques et la gestion des outils numériques, ainsi que les aspects juridiques et répressifs liés à la cybercriminalité.

Bien que les deux sites abordent la prévention de la cybercriminalité, E-Himaya se concentre sur la sensibilisation, la vérification des faits et la protection des enfants, tandis que Cybermalveillance se focalise sur la protection des données, la sécurité des systèmes et les aspects juridiques et répressifs. Ils offrent donc une complémentarité dans la couverture des différentes dimensions de la sécurité numérique.

3.3. *Analyse factorielle des correspondances (AFC)*

3.3.1. Présentation des résultats obtenus

Dans les deux sites, l'AFC permet de séparer nettement les classes et d'identifier leurs domaines d'intérêt distincts en matière de prévention de la cybercriminalité.

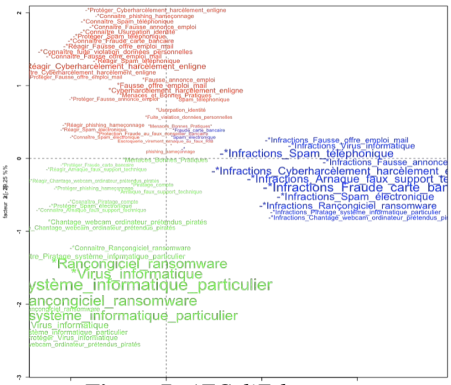

Figure 7. *AFC d'E-himaya*

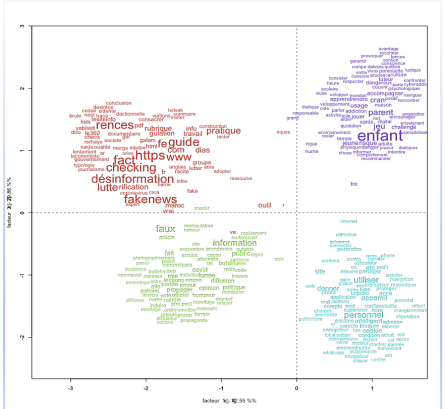

Figure 8. *AFC de* Cybermalveillance

Le contenu du site E-Himaya (Figure 7) :

- le premier facteur représente 42% de la masse du corpus. Il montre une nette séparation entre les classes 2 et 3 (abscisses positives) et la classe 1 (abscisse négative). Ce facteur reflète la distinction entre le domaine de la classe 1, qui se concentre sur la véracité de l'information, la lutte contre les fausses informations et la diffusion de l'information véridique, et les domaines des classes 2 et 3 qui se focalisent sur l'utilisation sécurisée des appareils numériques et la sensibilisation à la protection des enfants en ligne.

- le deuxième facteur représente 37,59% de la masse du corpus. Il met en évidence la distinction entre cette bipartition. Les classes 1 et 3 (ordonnées positives) sont nettement séparées de la classe 2 (ordonnée négative), tandis que la classe 1 apparaît moyennement centrée dans ce facteur.

Le contenu du site Cybermalveillance (Figure 8) :

- le premier facteur représente 60,75% de la masse du corpus. Il sépare de manière nette les classes 2 et 3 (abscisses négatives) de la classe 1 (abscisses positives). Ce facteur reflète la distinction entre le domaine de la sécurité des systèmes informatiques et la gestion des outils, d'une part, et les aspects juridiques et répressifs liés aux activités criminelles en ligne, d'autre part.

- le deuxième facteur représente 39,25% de la masse du corpus. Il met davantage en évidence la distinction entre cette bipartition. La classe 1 (ordonnée positive) est nettement séparée des classes 2 et 3 (ordonnées négatives), tandis que les classes 3 apparaissent plus centrées dans ce facteur.

3.3.2. Présentation des résultats obtenus par l'AFC

Dans le cas d'E-Himaya, l'AFC révèle trois zones distinctes sur le graphique de projection bidimensionnelle. La classe 1, associée à la véracité de l'information et à

la lutte contre les fausses informations, se situe en haut à gauche et est moyennement centrée. La classe 2, qui se concentre sur l'utilisation des appareils numériques, des logiciels et des réseaux, ainsi que la protection des informations personnelles, est isolée en haut à droite. La classe 3, axée sur la sensibilisation, l'éducation et la protection des enfants et des jeunes dans le contexte numérique, se trouve en bas à droite. Cette visualisation met en évidence les différences claires entre les classes et leurs domaines spécifiques d'intervention.

Pour Cybermalveillance, l'AFC montre également une séparation nette des classes dans l'espace bidimensionnel. La classe 1, liée à la protection des données personnelles et financières, est isolée en haut à droite. La classe 2, qui concerne la sécurité des systèmes informatiques et la gestion des outils, se trouve en bas à gauche. La classe 3, qui englobe les aspects juridiques et répressifs liés aux activités criminelles en ligne, est située en bas à droite. Cette visualisation met en évidence les caractéristiques distinctes des classes et leur spécialisation dans des domaines spécifiques de la prévention de la cybercriminalité.

3.4. *Analyse de similitude (ADS)*

3.4.1. Présentation des résultats obtenus

Dans le cas de l'ADS d'E-Himaya, plusieurs clusters thématiques émergent, s'articulant autour du terme « Information »

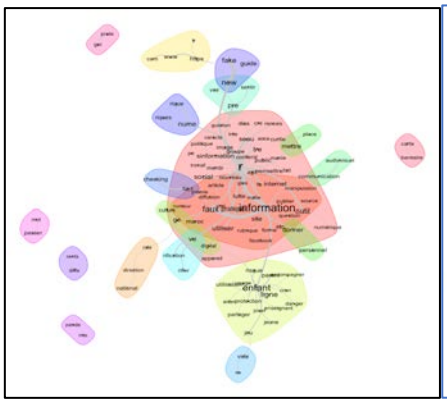

Figure 9. *ADS d'E-himaya*

Figure 10. *ADS de Cybermalveillance*

Pour le contenu E-Himaya (Figure 9), nous présenterons dans le tableau 1 les différents clusters, les termes associés et les thématiques qu'ils abordent.

Tableau 1. Clusters et termes associés d'E-Himaya

Cluster	Termes associés	Description
information	donner, permettre, communication, manipulation, personnel, audiovisuel, publier,	importance de la communication et diffusion d'informations fiables.
enfant	ligne, parent, internet, initiative, proposer, cadre, national, tuteur, direction, digital	protection et sécurité des données des enfants en ligne.
fake news	désinformation, lutte, outil, pratique, numérique, site, guide	lutte contre la désinformation et sécurité des transactions financières.
numérique	groupes, travail, risque	sécurité dans le domaine bancaire et prévention des fraudes financières.
faux	maroc, vrai, rubrique, facebook, permettre, diffusion	détection et lutte contre les contenus falsifiés, vérification des faits.
utiliser	appareil, sécurité, intelligent	utilisation sécurisée des appareils numériques et protection des données personnelles.
temps	culture, passer, mot	responsabilité légale et conséquences pour les auteurs de cybercriminalité.
paiement	paiement, carte, bancaire	transactions financières sécurisées.

Pour le contenu de Cybermalveillance (Figure 10), nous avons identifié différentes communautés lexicales associées aux concepts de « Victime » et « Donnée » dans le contexte de la cybersécurité. Une synthèse des domaines liés à chaque cluster est présentée dans le tableau 2.

Tableau 2. Clusters et termes associés de Cybermalveillance

Cluster	Thèmes abordés
données personnelles	protection des données, vie privée, sécurité de l'information, conformité réglementaire.
amende	législation, sanctions, conséquences juridiques, violations de la loi liées à la cybersécurité.
plaindre	justice, système judiciaire, signalement d'infractions, recours légal.
infraction	cybercriminalité, violations de la loi, types d'infractions cybernétiques.

bancaire	fraude bancaire, sécurité financière, protection des comptes en ligne, sécurité des transactions.
utiliser	utilisation des outils numériques, sécurité en ligne, vérification des adresses web.
message	communication en ligne, signalement de messages suspects, protection contre le phishing.
escroquerie	arnaques en ligne, tromperie, fraude sur internet.
demander	assistance, support technique, aide en matière de cybersécurité.
support	support technique, résolution de problèmes informatiques, bonnes pratiques de sécurité.
service	services en ligne, démarches administratives, sécurité des plateformes numériques.
appareil	sécurité des appareils électroniques, antivirus, protection contre les virus et les logiciels malveillants.
valeur	sécurité des transactions en ligne, protection des actifs numériques.
physique	sécurité des infrastructures physiques connectées, protection contre les attaques physiques.
bloquer	prévention des intrusions, sécurité du réseau, pare-feu.
contrôle	surveillance des activités, contrôle des accès, gestion des autorisations.
pirater	attaques de piratage, intrusion dans les systèmes, vulnérabilités de sécurité.
chantage	extorsion en ligne, menace de divulgation d'informations sensibles.
phishing	hameçonnage, techniques de manipulation en ligne, sensibilisation à la sécurité.

Les points de similarité entre les clusters thématiques des deux sites sont dans le tableau suivant (Tableau 3).

Tableau 3. Similarité entre les clusters thématiques des deux sites

Thème	Description
protection des données	les deux sites mettent en évidence l'importance de la protection et de la sécurité des données personnelles, avec des clusters tels que «donnée»(e-himaya) et « donnée » (cybermalveillance).
sécurité bancaire	les deux sites accordent une attention particulière à la sécurité des transactions financières et à la protection des comptes bancaires, avec des clusters tels que « numérique » (e-himaya) et « bancaire » (cybermalveillance).
communication sécurisée	les deux sites abordent la sécurité des communications électroniques et la prévention des tentatives de fraude ou

	d'hameçonnage, avec des clusters tels que « utiliser » (e-himaya) et « message » (cybermalveillance).
aspects juridiques	les deux sites soulignent l'importance de la responsabilité légale et des conséquences pour les auteurs de cybercriminalité, avec des clusters tels que « temps » (e-himaya) et « amende » (cybermalveillance).

Les points de différence entre les clusters thématiques des deux sites sont présentés dans le tableau 4.

Tableau 4. Similarité entre les clusters thématiques des deux sites

Thème	Description
protection des enfants en ligne	E-Himaya souligne la protection des enfants en ligne avec le cluster « Enfant », tandis que cette thématique n'est pas spécifiquement abordée dans les clusters de Cybermalveillance.
lutte contre la désinformation	E-Himaya accorde une attention particulière à la lutte contre la désinformation avec le cluster « Fake News », alors que ce sujet n'est pas directement mentionné dans les clusters de Cybermalveillance.
usage sécurisé des appareils numériques	E-Himaya souligne l'importance de l'utilisation sécurisée des appareils numériques avec le cluster « Utiliser », tandis que cette thématique n'est pas abordée spécifiquement dans les clusters de Cybermalveillance.
prévention des fraudes financières	E-Himaya se concentre sur la prévention des fraudes financières avec le cluster « Numérique », tandis que cette thématique est abordée de manière plus spécifique dans le cluster « Bancaire » de Cybermalveillance.

3.4.2. Présentation des résultats obtenus par l'AFC

Les deux sites se rejoignent sur des thématiques communes telles que la protection des données, la sécurité bancaire, la communication sécurisée et les aspects juridiques. Cependant, E-Himaya met davantage l'accent sur la protection des enfants en ligne, la lutte contre la désinformation et l'utilisation sécurisée des appareils numériques, tandis que Cybermalveillance se concentre plus spécifiquement sur la protection des comptes, les communications, les services en ligne et les aspects juridiques liés aux activités criminelles en ligne.

4. Stratégies discursives pour la lutte contre la cybercriminalité dans les deux sites

Le site E-Himaya adopte une stratégie discursive pédagogique et informative. Il est canalisé sur la sensibilisation en offrant des informations claires et concises sur les risques associés à la sécurité en ligne, en mettant particulièrement l'accent sur la protection des enfants contre les prédateurs en ligne. Dans le contexte de la médiatisation des cas de pédophilie, E-Himaya propose des conseils pour protéger les enfants des prédateurs en ligne. Le site fournit des informations sur les signes à reconnaître, les comportements à adopter et les précautions à prendre. En insistant sur la sensibilisation et l'éducation, E-Himaya cherche à renforcer la résilience des enfants et à leur offrir les compétences nécessaires pour se protéger contre les dangers en ligne. La protection des enfants en ligne est une responsabilité partagée entre les parents, les éducateurs, les gouvernements, les organisations et la société dans son ensemble. Les initiatives telles qu'E-Himaya fournissent des ressources et des conseils pour faire face à ces défis, mais la vigilance et la communication ouverte peuvent garantir une certaine sécurité des enfants sur Internet.

Cybermalveillance se focalise sur la protection des comptes en ligne, des communications et des aspects juridiques liés à la cybercriminalité, qui est de plus en plus présente dans la société numérique française. Les comptes bancaires, de messagerie et de réseaux sociaux constituent des cibles privilégiées pour les cybercriminels, et leur protection permet de prévenir le vol d'identité et la fraude financière. Les communications en ligne sont également vulnérables aux attaques et aux violations de la vie privée. La sécurisation des échanges d'informations, des courriers électroniques, des appels téléphoniques et des messages instantanés est donc une préoccupation majeure pour prévenir les atteintes à la confidentialité et à l'intégrité des données. Les services en ligne, qu'il s'agisse de plateformes de commerce électronique, de services bancaires en ligne ou de réseaux sociaux, sont souvent utilisés comme vecteurs d'attaques ou comme cibles pour l'exploitation de vulnérabilités. La protection de ces services peut prévenir les fraudes, les usurpations d'identité et autres abus en ligne. Enfin, les aspects juridiques liés aux activités criminelles en ligne permettent d'assurer la répression et la poursuite des cybercriminels. Comprendre les lois et les réglementations en matière de cybercriminalité, ainsi que les recours juridiques disponibles, est crucial pour lutter contre ces activités et protéger les victimes. Dans l'ensemble, Cybermalveillance s'intéresse à ces domaines clés afin de sensibiliser, d'informer et d'accompagner les utilisateurs dans la protection de leur vie numérique et de prévenir les risques associés à la cybercriminalité.

5. Questions non abordées dans les deux sites

Les résultats obtenus illustrent les stratégies discursives employées dans la prévention de la cybercriminalité. Cependant, certains aspects que nous considérons comme incommensurables dans ce discours sont omis.

5.1. *Omission de la dimension religieuse*

Suite à notre analyse, nous constatons que les sites E-Himaya et Cybermalveillance, bien qu'ils fournissent des ressources et des conseils essentiels en cybersécurité, présentent certaines lacunes dans leur approche. Une des principales lacunes est l'absence de prise en compte de la dimension religieuse et culturelle dans leur discours, alors que les religions et les médias s'articulent et que le populisme religieux au Maroc n'est pas seulement une pratique ressentie dans les médias, mais un fardeau politique et sociétal qui pèse lourdement sur les secteurs productifs et l'espace public (Bendahan, 2020). En se concentrant principalement sur les aspects techniques, juridiques et pratiques de la cybersécurité, ces sites ne tiennent pas compte des interactions potentielles entre la religion, la culture et la sécurité en ligne. Cela peut entraîner une compréhension partielle des motivations et des comportements des individus en matière de cybersécurité.

Par ailleurs, la médiatisation du religieux (Tudor et Bratosin, 2020, p. 3) obéit à des valeurs véhiculées par le cahier des charges des médias nationaux, mais la déformation du système médiatique a été amplifiée par l'explosion d'Internet, des réseaux sociaux et des chaînes satellitaires. Pour une approche plus inclusive, ces dimensions dans les analyses et les ressources proposées restent importantes. Cela permettrait de mieux répondre aux besoins spécifiques des communautés religieuses et culturelles, ainsi que de promouvoir une cybersécurité qui s'empare des problèmes de société au cœur de la cybercriminalité. L'identification de ces lacunes souligne l'importance d'une recherche future plus holistique qui intègre la dimension religieuse et culturelle dans l'étude de la cybersécurité.

Nous notons aussi l'absence de la mention du terrorisme dans les résultats obtenus, absence due à plusieurs facteurs. Tout d'abord, Cybermalveillance se concentre principalement sur la prévention et la lutte contre la cybercriminalité, qui englobe un large éventail d'activités illégales en ligne telles que le vol d'identité, la fraude en ligne, le phishing, les attaques de logiciels malveillants, etc. Le terrorisme, bien qu'il puisse avoir des ramifications en ligne, est un domaine spécifique et complexe qui relève souvent de la compétence des agences de sécurité nationale et des organismes spécialisés dans la lutte contre le terrorisme. La prévention et la lutte contre le terrorisme impliquent des mesures de sécurité plus larges qui dépassent souvent le cadre de la cybercriminalité et nécessitent une coordination et une coopération internationales.

Cela dit, Cybermalveillance peut fournir des informations et des conseils généraux sur la sécurité en ligne qui peuvent également être pertinents dans le contexte de la lutte contre le terrorisme en ligne. Par exemple, la sensibilisation aux pratiques de sécurité en ligne, la protection des comptes et des données personnelles, et la prévention des attaques de phishing peuvent être des préoccupations pertinentes dans la prévention de l'exploitation terroriste en ligne.

Conclusion

Notre étude comparative des approches de prévention de la cybercriminalité sur les sites E-Himaya (Maroc) et Cybermalveillance (France) a révélé l'intérêt des stratégies discursives numériques dans la lutte officielle contre la cybercriminalité, tant au Nord qu'au Sud. Ainsi, E-Himaya et Cybermalveillance adoptent des approches qui, bien que distinctes, sont complémentaires. Le contenu E-Himaya se concentre sur la sensibilisation des jeunes, en abordant des thèmes tels que la désinformation et la protection des enfants, tandis que le contenu de Cybermalveillance privilégie la sécurité et la conformité réglementaire en matière de données personnelles et financières.

Cependant, malgré cette complémentarité, certaines limites doivent être soulignées. D'une part, les deux sites négligent la dimension religieuse et culturelle, qui peuvent influencer la perception et la réponse des utilisateurs face aux menaces en ligne. D'autre part, la question du terrorisme, indéniablement liée à la cybercriminalité, n'est pas abordée par Cybermalveillance, ce qui pourrait priver les utilisateurs d'une compréhension complète des enjeux de sécurité numérique.

Bien que ces plateformes fournissent des ressources importantes pour sensibiliser et protéger contre la cybercriminalité, il convient de considérer ces dimensions manquantes pour enrichir le discours sur la sécurité en ligne. De futures recherches pourraient examiner ces aspects afin de développer des stratégies plus globales et inclusives pour combattre la cybercriminalité dans toute sa complexité.

Références

Alauzen, M. (2024) . Anne Bellon, L'État et la toile. Des politiques de l'internet à la numérisation de l'action publique, Vulaines-sur-Seine, Éditions du Croquant, 2022, 319 p. Réseaux, N° 243(1), 335-339. https://doi.org/10.3917/res.243.0335.

Bendahan, M., & Akhiate, Y. (2020). Religious Media in the Maghreb : What Are the Boundaries between the Public and Private Spheres? Religions, 11(12), 638. https://doi.org/10.3390/rel11120638

Bisiani, F. (2020). *Pour une approche discursive de la terminologie européenne et nationale, en français et en espagnol, des textes non contraignants sur les politiques sécuritaires* (2001-2018). [Thèse de doctorat, Linguistique, Université Paris Cité ; Università degli studi (Udine, Italie); Università degli studi (Trieste, Italie)]. Français. https://tel.archives-ouvertes.fr/tel-03185475

Bougren, G., & Chadi, M. (2023). La cybercriminalité dans l'ère numérique: Une étude des défis juridiques et réglementaires. International Journal of Innovation and Scientific Research, 68(1), 40-49.

Brenner, S. W., & Koops, B. J. (2004). Approaches to cybercrime jurisdiction. Journal of High Technology Law, 4(1). https://ssrn.com/abstract=786507

Brotcorne, P. et al. (2010). Diversité et vulnérabilité dans les usages des TIC. La fracture numérique au second degré. Academia Press.) (ISBN:9789038216980) 239 pages http://hdl.handle.net/2078.1/129028

Charaudeau, P. (2009). Dis-moi quel est ton corpus, je te dirai quelle est ta problématique. Corpus, (8), P.63.

Chawki, M. (2006). Essai sur la notion de cybercriminalité. IEHEI. p. 6.

Chirwa, D., & Ncube, C. (Eds.). (2023). The Internet, Development, Human Rights and the Law in Africa (1st ed.). Routledge. https://doi.org/10.4324/9781003308157

Daghmi, F., Toumi, F., & Amsider, A. (2013). Les médias font-ils les révolutions ? Regards critiques sur les soulèvements arabes. L'Harmattan

Daghmi,F., Amsidder,A, & Toumi, F. (2012), La mobilisation sociale à l'ère des réseaux Sociaux-Cas du Maroc.Essachess, Vol. 5, No 1(9)

De Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness : The need for evidence-based framing strategies. Government Information Quarterly : an international journal of information technology management, policies, and practices, 34(1), 1-7. https://doi.org/10.1016/j.giq.2017.02.007

Décary-Hétu, D. (2020). La cybercriminalité. CrimRxiv.

Fairclough, N. (2003). Analysing discourse: Textual analysis for social research. Routledge.

Ghernaouti, S. (2023). Cybercriminalité : Comprendre. Prévenir. Réagir. https://shs.cairn.info/cybercriminalite-comprendre-prevenir-reagir--9782100858699?lang=fr.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2, 13–20. https://doi.org/10.1007/s11416-006-0015-z

Granjon, F. (2018) . Mouvements sociaux, espaces publics et usages d'internet. Pouvoirs, N° 164(1), 31-47. https://doi.org/10.3917/pouv.164.0031.

Haounani, A., & Akkour, S. (2023). Les données personnelles à l'ère du big-data : quel cadre juridique au Maroc ?. Revue Internationale du Chercheur, 4, 1. https://doi.org/10.21428/cb6ab371.9e0bdd09

Jewkes, Y., & Yar, M. (2010). Introduction : the internet, cybercrime and the challenges of the twenty-first century. In Y. Jewkes, & M. Yar (Eds.), Handbook of Internet Crime (pp. 1–15). Willan Publishing.

Joissains, S., & Bigot, J. (2020). Rapport d'information sur la lutte contre la cybercriminalité (N° 613). Sénat, session extraordinaire de 2019-2020. Commission des affaires européennes et Commission des lois. Enregistré à la Présidence du Sénat le 9 juillet 2020.

Khelifi, H. (2016). La lexicométrie : un outil efficient pour l'analyse du discours. Dans Médias numériques, langues, discours, pratiques et interculturalité : Actes du Colloque international (pp. 151-161). Université Paris 8 Vincennes-Saint-Denis, Université Grenoble Alpes; Université Ibn Zohr. https://hal.archives-ouvertes.fr/hal-01730406

Leblanc, J.-M., & Pérès, M. (2011). Propositions de visualisations pour la navigation lexicométrique. Document numérique, 14, 105–134. https://www.cairn.info/revue--2011-1-page-105.htm. P.2

Leman-Langlois, S. (2006). Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace commercial. Criminologie, 39(1), 63–81. https://doi.org/10.7202/013126ar

Menusier, A. (2021). Figure du Hirak algérien, Kaddour Chouicha, encerclé par le pouvoir, témoigne. Le Regard Libre, (6), 18-19.

Moussaoui-Bournane, F., & Clavel, S. (2007). La communication : un des piliers de la prévention. Dans H. Sancho-Garnier (Éd.), Au-delà de l'information, la prévention : Dépistage et cancer (pp. 123-140). Springer. https://doi.org/10.1007/978-2-287-33281-4_3

Pereira, B (2016). La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité. Revue internationale de droit économique, 2016/3 t. XXX. pp. 387-409. https://doi.org/10.3917/ride.303.0387

Perwej, Y., Abbas, Q., Dixit, J., Akhtar, N., & Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. International Journal of Scientific Research and Management, 9(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences, 2(2), 379-398, P.385. https://doi.org/10.3390/forensicsci2020028

Poudat, C., & Landragin, F. (2017). Explorer un corpus textuel. Méthodes – pratiques – outils. De Boeck Supérieur. P.25. ISBN : 978-2-8073-0563-2

Proulx, S. (2020). La participation numérique : Une injonction paradoxale. Presses des Mines.

Schell, B. H. & C. Martin. (2004). Cybercrime: A Reference Handbook. Santa Barbara, États-Unis . Retrieved from http://publisher.abc-clio.com/9781851096886

Tudor, M.-A., & Bratosin, S. (2020). Croire en la technologie. Communication, 37(1). Consulté le 23 septembre 2024, à partir de http://journals.openedition.org/communication/11021

Wall, D.S. (2024) Cybercrime: The Transformation of Crime in the Information Age, 2nd edition,Cambridge, Cambridge: Polity. ISBN-10: 0745653529 / ISBN-13: 978-0745653525

Wybo, J., Gouttas, C., Ok, É., & Lions, P. (2015). L'impact des réseaux sociaux dans la gestion des crises et le cybercrime. Sécurité et Stratégie, 18, 37–43. https://doi.org/10.3917/sestr.018.0037