

Content available at: <https://www.ipinnovative.com/open-access-journals>IP International Journal of Forensic Medicine and
Toxicological SciencesJournal homepage: <http://www.ijfmts.com/>

Original Research Article

The dark web: A hidden menace or a tool for privacy protection

Gurleen Kaur ^{1*}, Debhjit Mukherjee ², Bhavika Moza ², Vaishali Pahwa ²,
Kulwinder Kaur ², Kamaljeet Kaur ²¹Dept. of Forensic Science, RIMT University University, Punjab, India²Dept. of Forensic Science, Chandigarh University, Punjab, India

ARTICLE INFO

Article history:

Received 16-11-2023

Accepted 20-12-2023

Available online 19-01-2024

Keywords:

Cybercriminals

Whistle blowers

Environment

ABSTRACT

Background: The dark web has long been a subject of debate, as it raises questions about its covert threats and privacy safeguarding capabilities. It's an internet realm requiring specific software or authorization, notorious for illegal activities and untraceable transactions. Researchers and law enforcement agencies use the dark web for intelligence gathering on cybercriminals, making it crucial in understanding the evolution of the internet and emerging criminal activities. Additionally, studying the dark web helps identify cybersecurity threats and vulnerabilities.

Aim: This research explores the relationship between the dark web and mental health, investigating the public's perception of the dark web as both a hidden menace and a tool for privacy protection. The primary aim is to examine the correlation between public perception and engagement in dark web services, while also exploring potential mental health ramifications.

Materials and Methods: To collect data, we conducted a survey among university students and regular internet users. The research process involved identifying 18 research questions covering topics such as dark web knowledge, usage frequency, security measures, awareness of government regulations, ability to differentiate legal and illegal content, transaction methods, and understanding the dark web's role in promoting freedom of speech. We collected 158 responses from different departments of Chandigarh University, removing duplicates to retain 156 responses meeting our criteria. Data was compiled in an Excel file for further statistical evaluation.

Result and Discussion: While the dark web is not widely accessed, users may experience psychological consequences due to its association with cybercrime, disturbing content, and radicalization. This connection leads to heightened anxiety, fear, and distress among users. Concerns about privacy, security, and associated risks further contribute to these apprehensions. Motivations for dark web access, such as curiosity and anonymity, may stem from underlying psychological factors. However, navigating illegal and potentially harmful content can result in emotional turmoil, moral dilemmas, guilt, or shame. These findings highlight the need for public awareness campaigns, educational initiatives, and targeted interventions promoting mental well-being and safe internet practices. Enhancing individuals' knowledge about the dark web's risks and potential psychological consequences empowers them to make informed decisions and protect their mental health in the digital age.

This is an Open Access (OA) journal, and articles are distributed under the terms of the [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 License](https://creativecommons.org/licenses/by-nc-sa/4.0/), which allows others to remix, tweak, and build upon the work non-commercially, as long as appropriate credit is given and the new creations are licensed under the identical terms.

For reprints contact: reprint@ipinnovative.com

1. Introduction

The internet is a vast and ever-expanding network of information that connects people and businesses across the

* Corresponding author.

E-mail address: gurleen2597@gmail.com (G. Kaur).

world. The internet is made up of three main parts, namely surface web, deep web, and dark web. The surface web is the part of the internet that is easily accessible through standard search engines like Google and yahoo. The deep web refers to the part of the internet that is not indexed by search engines and can only be accessed through specific tools like password-protected websites or online databases. Lastly, the dark web is the part of the internet that requires specific software or authorization to access, and it is infamous for being a hub for illegal activities and criminal transactions without the risk of being tracked or identified.¹⁻⁴

The dark web is a subset of the deep web that is intentionally hidden and inaccessible through regular browsers. It is accessible only through specific software like TOR (The Onion Router), which allows users to browse the internet anonymously. It also serves as a platform for criminals to communicate and organize illegal activities.^{5,6}

The study of the dark web is crucial in understanding the evolution of the internet and the emergence of new criminal activities. Researchers and law enforcement agencies use the dark web to gather intelligence on cybercriminals and monitor their activities. Additionally, studying the dark web can also help to identify potential threats and vulnerabilities in cybersecurity systems. Researchers can use network analysis to identify patterns of communication between users and uncover hidden markets or forums. Additionally, forensic linguistics can be used to identify the language and writing style of individuals who engage in illicit activities on the dark web.⁷

Dark web also has some advantages, it provides a secure platform for whistle blowers, activists, and journalists to communicate and exchange information without fear of government surveillance or censorship.^{8,9}

However, the use of the dark web also has its risks, especially for users who engage in illegal activities. Since the dark web operates outside of the law, users are susceptible to scams, fraud, and cyberattacks. Additionally, the use of the dark web can also expose users to malware and viruses, which can compromise their personal information and cause irreparable damage to their devices. User's data is stolen, eventually that data is sold. The stolen data is purchased by criminals for identity theft, financial fraud, or other illegal activities.⁴⁻¹²

Drugs, firearms smuggling, and human trafficking are among some of the crimes committed in dark web platform. Illegal drugs, such as cocaine, heroin, and methamphetamine, as well as prescription drugs, such as opioids are sold. The anonymity of the dark web allows drug dealers to operate without fear of being caught by law enforcement. The dark web provides a platform for the sale of a wide range of weapons, including firearms, ammunition, and explosives. These weapons are often sold to individuals who are not legally allowed to possess them, such as convicted felons or individuals with a history of

mental illness. Human trafficking is another illegal service provided by the dark web. Criminals can use the dark web to advertise and sell individuals for forced labor or sexual exploitation. This is a particularly heinous crime, and law enforcement agencies around the world are working to combat human trafficking on the dark web. While law enforcement agencies and officials are dedicatedly working to combat these illegal activities, the dark web incognito environment makes it challenging for investigators.^{13,14}

Forensic significance is another area of interest when studying the dark web. Law enforcement agencies can use forensic tools and techniques to analyze the digital footprints left behind by cybercriminals on the dark web. These digital footprints can provide valuable evidence in investigations, including the identification of suspects, recovery of stolen data, and prevention of future crimes.¹²⁻¹⁵ The dark web is a part of the internet that remains shrouded in mystery and controversy. While it has its advantages, the dark web is primarily associated with criminal activities and illicit transactions. Nonetheless, the study of the dark web is crucial in understanding the evolution of the internet and the emergence of new criminal activities. Additionally, the dark web's forensic significance cannot be ignored, as it provides valuable evidence in cybercrime investigations.

The dark web constitutes a clandestine segment of the internet that remains beyond the purview of conventional search engines. Accessible solely through specialized software such as TOR (The Onion Router), this enigmatic digital realm is frequently linked with illicit endeavors like narcotics trade and cyber intrusions. However, it is imperative to recognize that the dark web also serves legitimate functions, notably safeguarding individuals' privacy. The use of the dark web has been a topic of debate, with some viewing it as a hidden menace that facilitates illegal activities and others seeing it as a tool for protecting privacy and free speech. Certainly, the dark web can serve as a nexus for cyber malefactors, facilitating nefarious enterprises such as the trafficking of narcotics, weaponry, and pilfered data. Conversely, the dark web can also serve as an arena where individuals can engage in covert communication, fortify their online anonymity, and acquire information free from the specter of censorship.

In this context, it is of paramount significance to delve into the role of the dark web within our digital milieu, along with the prospective advantages and perils inextricably tied to its utilization. While the dark web poses formidable quandaries for law enforcement and policymakers, it concurrently harbors the potential for individuals and entities to safeguard their privacy and exercise their freedom of expression in an ever-more interlinked and surveilled global landscape.

2. Objective

The primary aim of this survey-based research paper is to conduct a thorough investigation into the public’s perception concerning the dark web and its correlation with the engagement in dark web services, all the while delving into the potential ramifications for mental well-being.

3. Materials and Methods

The article aims to explore the public perception of the dark web, specifically examining whether it is perceived as a hidden threat or a tool for safeguarding privacy. To gather data for the article, a Google survey was conducted among university students and regular internet users. The research process involved identifying the research question, determining appropriate data sources and search methods, setting inclusion and exclusion criteria, extracting data, and analyzing and synthesizing the information.

Modalities employed within the dark web can encompass a diverse spectrum of undertakings, comprising the illicit trade in contraband such as narcotics and armaments, alongside the dissemination of confidential and sensitive information and data. While these activities undeniably constitute a threat, it is imperative to underscore that the dark web can also function as a mechanism for the preservation of privacy. Nevertheless, caution is advised when navigating the dark web, given the prevalence of illegal activities and scams. It is crucial to exercise caution and adopt appropriate measures to safeguard privacy and security while accessing the dark web. Ultimately, whether the dark web is perceived as a hidden menace or a tool for privacy protection depends on its usage.

Figures 1 and 2 comprise 18 questions related to the dark web, enabling us to gather information from both dark web users and non-users, as well as assess the general awareness levels surrounding the dark web. Understanding the various types of dangers present on the dark web can help reveal how illicit services and materials are utilized and their subsequent implications. Consequently, this highlights the importance of advancing technologies and law enforcement efforts to track down criminals. Identifying the techniques, tools, and technologies employed by law enforcement to apprehend individuals operating on the dark web will guide future actions. The collaboration between law enforcement and advanced technologies will work in tandem to undermine the plots of cybercriminals.

Strategic guidelines and electronic searches were conducted across various databases such as ScienceDirect, Springer, ACM Digital Library, and Google Scholar to collect relevant data for the review paper. A total of 158 forms were collected within different departments of Chandigarh University, but duplicates were removed, resulting in a reduced number of 156 responses that met the criteria for the article. An Excel file was created

based on the responses collected from the Google form, encompassing information pertaining to knowledge of the dark web, frequency of usage, security measures employed during access, awareness of government regulations, ability to distinguish between illegal and legal content on the dark web, modes of transaction, and awareness of the dark web’s role in promoting freedom of speech and expression. Even, Excel analysis tool was used to convert the data in to percentages. The data includes different questions regarding people’s perspectives on the dark web, and some parameters were combined and presented in a single graph. E.g., Figure 3 graphically represents the responses in terms of "yes" or "no" across different parameters.

3.1. Survey

https://docs.google.com/forms/d/e/1FAIpQLSejdrLEUYvJuvMuMkX2ozGTUyx5pFzEzKcp85NxmJ-4goLIw/viewform?usp=sf_link

4. Result

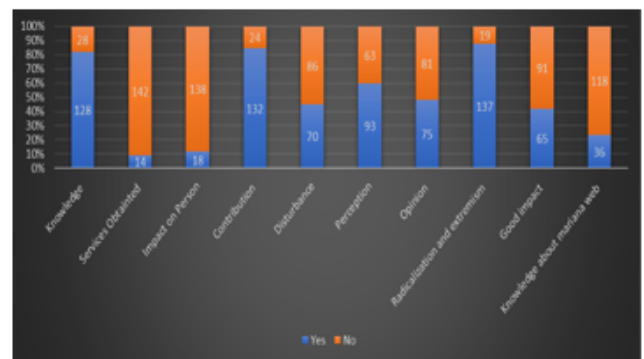


Figure 3: People’s Perspectives on the dark web with respect to different parameter

Figure 3 reveals that approximately 80% of individuals are aware of the dark web, with a majority holding a negative perception of its effects on individuals and society. Only ten percent of participants reported using the dark web, while a larger percentage associated it with cybercrime and illegal activities. The data indicates a consensus among respondents, with around 82% believing the dark web contributes to cybercrime, while approximately 18% hold a contrary view. Disturbing content was perceived by 42% of participants, highlighting its subjective nature. About 59% of respondents expressed the opinion that the dark web should be subject to stricter government regulations, while 41% opposed this view, emphasizing the ongoing debate over regulation. The data also showed widespread concern, with 88% believing the dark web contributes to online radicalization and extremism. Conversely, 41% believed that the benefits of the dark web outweigh the

A SURVEY FOR A STUDY ON IMPACTS OF DARK WEB ON MODERN SOCIETY.

Name: _____ Mail id: _____

1. Have you ever heard of the Dark Web?
a. Yes
b. No

2. How frequently do you access the Dark Web?
a. Daily
b. Weekly
c. Monthly
d. Rarely
e. Never

3. What is the primary reason for accessing the Dark Web?
a. Anonymity
b. Purchasing illegal goods
c. Freedom of speech
d. Other

4. Have you ever witnessed or been a victim of cybercrime on the Dark Web?
a. Yes
b. No

5. What is your perception of the Dark Web?
a. Dangerous
b. Useful
c. Neutral
d. Other

6. Do you think the Dark Web is contributing to an increase in cybercrime?
a. Yes
b. No

7. How concerned are you about the privacy and security risks associated with accessing the Dark Web?
a. Very concerned
b. Somewhat concerned
c. Not concerned
d. Other

Figure 1: Survey questions for understanding perception of dark web among people

A SURVEY FOR A STUDY ON IMPACTS OF DARK WEB ON MODERN SOCIETY.

8. Do you think law enforcement agencies are doing enough to combat cybercrime on the Dark Web?
a. Yes
b. No

9. What measures do you take to protect your privacy and security when accessing the Dark Web?
a. VPN
b. Tor browser
c. Anti-virus software
d. Other

10. Have you ever come across content on the Dark Web that made you uncomfortable or disturbed?
a. Yes
b. No

11. What is your opinion on the role of the Dark Web in promoting freedom of speech and expression?
a. Positive
b. Negative

12. Do you think the Dark Web should be more closely regulated by governments?
a. Yes
b. No

13. How important do you think it is for individuals to be educated about the risks associated with accessing the Dark Web?
a. Very important
b. Somewhat important
c. Not important
d. Other

14. Do you think the Dark Web is contributing to an increase in online radicalization and extremism?
a. Yes
b. No

15. How confident are you in your ability to differentiate between legal and illegal content on the Dark Web?
a. Very confident
b. Somewhat confident
c. Not confident
d. Other

16. What is your opinion on the use of cryptocurrencies as a means of payment on the Dark Web?
a. Positive
b. Negative

A SURVEY FOR A STUDY ON IMPACTS OF DARK WEB ON MODERN SOCIETY.

17. Do you think the benefits of the Dark Web outweigh the risks and negative impact on society?
a. Yes
b. No

18. Have you heard about Mariana Web?
1. Yes
2. No

Figure 2: Survey questions for understanding perception of dark web among people

risks, while the majority had concerns about its negative impact. Furthermore, most people, approximately 78%, were unaware of the Mariana Web, indicating limited knowledge about this concept. Overall, the data provides insights into public perceptions of the dark web, including concerns about cybercrime, disturbance caused by content, the need for regulation, the association with extremism, and limited awareness of specific aspects such as the Mariana Web.

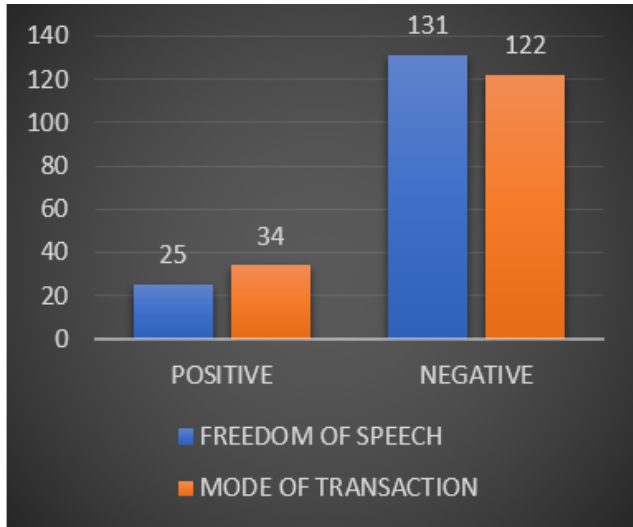


Figure 4: People perspective on freedom of speech and mode of transaction by dark web

Figure 4 presents data from 156 individuals regarding their views on the dark web’s role in promoting freedom of speech and expression and the use of cryptocurrencies for transactions. The majority (84.0%) disagreed that the dark web promotes freedom of speech and expression, while a minority (16.0%) held the opposite view. In terms of cryptocurrencies as a mode of transaction on the dark web, a significant majority (78.2%) believed it has a negative impact, while a smaller minority (21.8%) disagreed. Overall, the data indicates a prevailing perception that the dark web does not promote freedom of speech and expression, and there are concerns about the negative impact of cryptocurrencies for transactions on the platform.

Based on the data from Figure 5, it can be concluded that the majority of individuals (71.1%) have never accessed the dark web. This indicates that the dark web is not widely used, with many individuals either unaware of its existence or having no need to access it. Among those who do access the dark web, only a small minority (3.8%) do so on a daily basis, while the rest access it less frequently. Most individuals (19.8% rarely, 4.4% weekly, and 0.64% monthly) use the dark web infrequently, suggesting that it is not a vital platform for them and is only utilized on occasion for specific purposes.

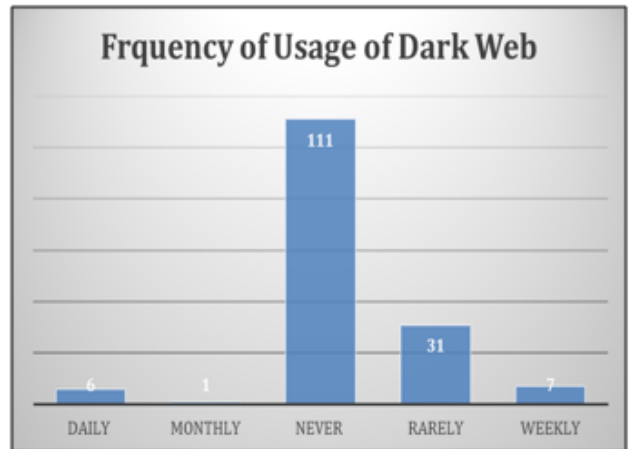


Figure 5: Uses of dark web

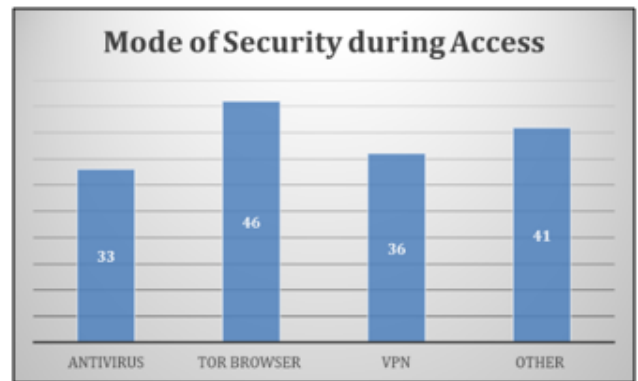


Figure 6: Security during access

Based on the data from Figure 6, it can be concluded that a significant number of individuals take steps to safeguard their privacy and security when accessing the dark web. The most commonly employed measure is the use of Tor Browser, with nearly one-third of individuals (29.4%) utilizing it. This indicates that individuals are aware of the potential risks associated with accessing the dark web and are actively seeking ways to protect their privacy and security. Additionally, a smaller portion of individuals (23%) opt for a VPN (Virtual Private Network) to enhance their privacy and security while accessing the dark web. VPNs are a widely recognized tool for online privacy and security, making their use in the context of the dark web understandable. Notably, a substantial percentage of individuals (21.1%) employ other undisclosed measures to safeguard their privacy and security while accessing the dark web. Although the specific nature of these measures is not provided, it suggests that there are alternative tools and techniques individuals rely on for protection. Finally, a relatively large proportion of individuals (26.2%) did not specify the measures they take to protect their privacy and

security.

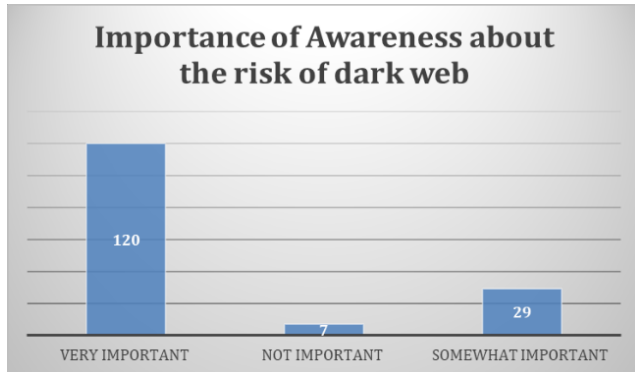


Figure 7: Awareness of the risks related to dark web

According to the data in Figure 7, the majority of individuals (76.9%) recognize the importance of educating people about the risks associated with accessing the dark web. This indicates that individuals are aware of the potential dangers and believe that raising awareness is crucial. A smaller percentage (18.5%) consider it somewhat important to educate individuals about these risks. However, a very small minority (4.4%) do not view it as important to educate individuals about the risks associated with accessing the dark web. This could be attributed to a lack of awareness or understanding regarding the potential hazards involved.

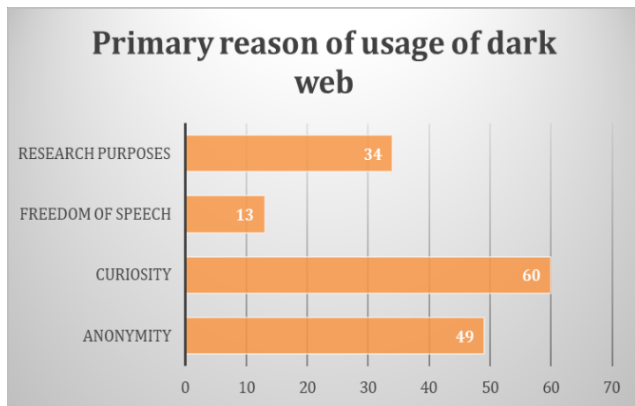


Figure 8: Primary reasons of usage of dark web

According to the data in Figure 8, individuals have varying opinions regarding the primary reasons for accessing the dark web. The largest percentage (38.4%) consider curiosity as the main motivation, indicating a desire to explore and uncover the offerings of the dark web. A significant portion (31.4%) view anonymity as the primary reason, aligning with the common association of the dark web with privacy and anonymity. A smaller proportion (21.7%) believe research to be the primary reason, suggesting legitimate academic or investigative

purposes. Lastly, a very small minority (8.3%) attribute accessing the dark web to a pursuit of freedom of speech.

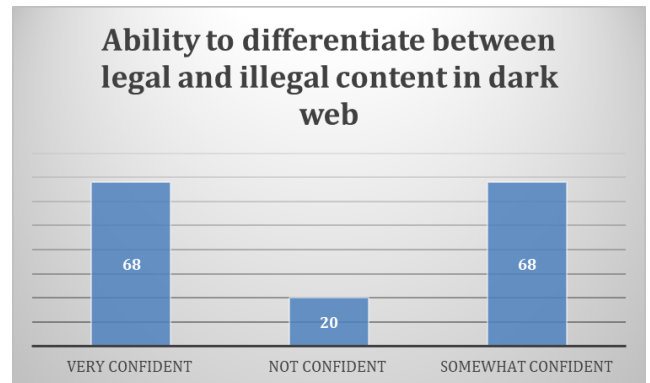


Figure 9: Differentiating ability between a legal and illegal content

Figure 9 data indicates that a significant majority of individuals (87%) have some level of confidence in their ability to differentiate between legal and illegal content on the dark web. However, it is noteworthy that approximately 12.8% express a lack of confidence in making this distinction. Among the respondents, around 43.5% exhibit a high level of confidence in their ability to discern legal from illegal content, suggesting their well-informed understanding of the dark web and associated risks. Additionally, an equal proportion (43.5%) report being somewhat confident, potentially indicating a recognition of the complexity involved or a need for further knowledge and experience in this domain.

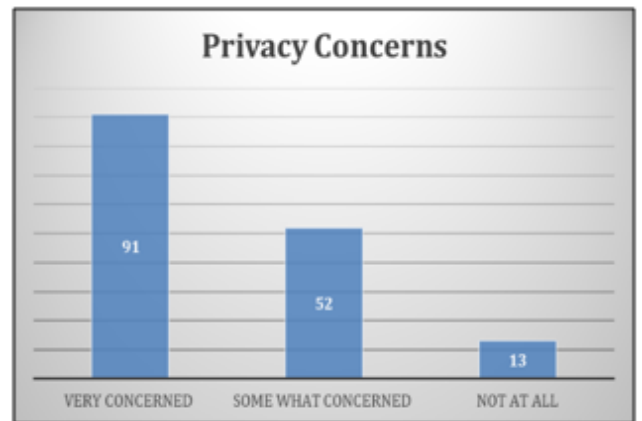


Figure 10: Privacy concerns of people

Figure 10 data reveals that a majority of individuals (58.3%) express concerns regarding privacy, security, and risks associated with accessing the dark web. This indicates their awareness of potential risks and their proactive approach to self-protection. A significant proportion (33.3%) demonstrate some level of concern, suggesting an awareness of risks but a potential need for further

protective measures. A small minority (8.3%) show no concern regarding privacy, security, and risks associated with accessing the dark web. Overall, the data highlights varying levels of concern among individuals, with the majority expressing some level of worry.

5. Discussion

The data presented in Figures 3 to 10 provides valuable insights into public perceptions, behaviors, and concerns regarding the dark web. These findings can be used to explore the potential link between dark web usage and mental health.

One notable observation from the data is that a relatively small percentage of individuals reported accessing the dark web (10% according to (Figure 3)). This suggests that the dark web is not widely used, and the majority of individuals may not be aware of its existence or may not have a need to access it. This finding could imply that the impact of dark web usage on mental health may be limited to a smaller subset of the population.

Considering the negative perception associated with the dark web, as indicated by Figures 3 and 4, it is reasonable to assume that individuals who engage with the dark web might experience certain psychological implications. The association of the dark web with cybercrime, disturbing content, and online radicalization, as highlighted in the data, may contribute to increased anxiety, fear, and psychological distress among users. The concerns expressed by respondents in Figures 10 and 7 regarding privacy, security, and the risks associated with accessing the dark web further support this notion.

Moreover, the reasons provided for accessing the dark web in Figure 8, such as curiosity and anonymity, could also be indicative of underlying psychological factors. Curiosity may drive individuals to explore the unknown, but it could also stem from a desire for novelty or escapism. Anonymity, which is commonly associated with the dark web, may attract individuals seeking to maintain privacy or engage in activities they would not openly participate in. These motivations, while not inherently negative, can have implications for mental well-being, depending on the individual's intent and experiences within the dark web.

It is important to acknowledge that accessing the dark web involves navigating through illegal and potentially harmful content. The data indicates that individuals are aware of the risks associated with the dark web (Figures 3 and 7) and take measures to protect their privacy and security (Figure 6). However, the ability to differentiate between legal and illegal content on the dark web is not universal (Figure 9). This lack of certainty and the potential exposure to disturbing or illicit material could have psychological consequences, including distress, moral dilemmas, and feelings of guilt or shame.

While the available data provides insights into public perceptions and behaviors related to the dark web, it does not provide a direct measurement of mental health outcomes. To establish a robust link between dark web usage and mental health, further research is necessary. Longitudinal studies, qualitative interviews, and psychological assessments can provide a more comprehensive understanding of the psychological impact of dark web usage.¹⁶

So basically, the data suggests that dark web usage may be associated with psychological implications, particularly in terms of anxiety, fear, and distress. The negative perception, concerns about privacy and security, and the potential exposure to disturbing or illegal content all contribute to this link. This information can be valuable for informing public awareness campaigns, educational initiatives, and interventions aimed at promoting mental well-being and safe internet practices.¹⁷

6. Conclusion

In conclusion, the survey research article on the dark web provides important insights into public perceptions and behaviors regarding its usage and its potential impact on mental health. The data suggests that the dark web is not widely accessed, but those who do engage with it may experience psychological implications. The association of the dark web with cybercrime, disturbing content, and online radicalization can contribute to increased anxiety, fear, and distress among users. Concerns about privacy, security, and the risks associated with accessing the dark web further support this notion.^{4,10–12}

Motivations for accessing the dark web, such as curiosity and anonymity, may have underlying psychological factors. However, navigating through illegal and potentially harmful content poses risks and can lead to distress, moral dilemmas, and feelings of guilt or shame. While individuals are aware of these risks and take measures to protect their privacy and security, the ability to differentiate between legal and illegal content on the dark web is not universal.^{13–18}

It is important to note that the available data does not directly measure mental health outcomes, and further research is needed to establish a robust link between dark web usage and mental health. Longitudinal studies, qualitative interviews, and psychological assessments can provide a more comprehensive understanding of the psychological impact of dark web usage.

Overall, the findings highlight the need for public awareness campaigns, educational initiatives, and interventions to promote mental well-being and safe internet practices.¹⁹ By enhancing individuals' knowledge about the risks and potential psychological implications of the dark web, we can empower them to make informed decisions and protect their mental health in the digital age. Balancing the advantages and risks of the dark web is

crucial, and prioritizing mental well-being and safe online practices is essential in today's digital era.

7. Source of Funding

None.

8. Conflict of Interest

None.

Acknowledgments

All authors contributed equally to the research


References

1. Tavabi N, Bartley N, Abeliuk A, Soni S, Ferrara E, Lerman K. Characterizing activity on the deep and dark web. *Companion proceedings of the 2019 world wide web conference*. 2019;p. 206–19.
2. Hurlburt G. Shining light on the dark web. *Computer*. 2017;50(4):100–5.
3. Bradbury D. Unveiling the dark web. *Network security*. 2014;2014(4):14–21.
4. Finklea KM. Dark web. Congressional Research Service; 2015. Available from: <https://sgp.fas.org/crs/misc/R44101.pdf>.
5. Thomaz F, Salge C, Karahanna E, Hulland J. Learning from the Dark Web: leveraging conversational agents in the era of hyper-privacy to enhance marketing. *J Acad Mark Sci*. 2020;48:43–63.
6. The Future of Dark Web. Available from: <https://www.soscanhelp.com/blog/future-of-the-dark-web>.
7. Chen I, Tortosa C. The use of digital evidence in human trafficking investigations. *Anti-trafficking Rev*. 2020;p. 122–6.
8. Gehl RW. Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media Soc*. 2016;18(7):1219–54.
9. Beckstrom M, Lund B. Casting light on the Dark Web: A guide for safe exploration. Rowman & Littlefield; 2019. p. 132.
10. Crisp J. Use and Abuse of Social Media in Human Trafficking. *J Am Acad Child Adolesc Psychiatry*. 2021;60(10):80.
11. Jardine E. Online content moderation and the Dark Web: Policy responses to radicalizing hate speech and malicious content on the Darknet First Monday. 2019;.
12. Chertoff M, Simon T. The impact of the dark web on internet governance and cyber security; 2015. Available from: <https://www.cigionline.org/publications/impact-dark-web-internet-governance-and-cyber-security/>.
13. Vogt SD. The digital underworld: Combating crime on the dark web in the modern era. *L*. 2017;15:104–104.
14. Dixon HB. Human trafficking and the internet (and other technologies, too). *Judges J*. 2013;52:36.
15. Romeo AD. Hidden threat: the dark web surrounding cyber security. *N Ky L Rev*. 2016;43:73–73.
16. Vlassov V, Meilahs P, Soshnikov S, Idrisov B. Illegal drug sales in the mirror of the dark web marketplace. *Eur J Public Health*. 2021;31(3):165–266.
17. Benzon K. Depression and narrative: Telling the dark; 2008.
18. Carr T, Zhuang J, Sablan D, Larue E, Wu Y, Hasan A. Into the Reverie: Exploration of the Dream Market. *IEEE Int Conf Big Data (Big Data)*. 2019;p. 1432–73.
19. Munk T. Policing virtual spaces: public and private online challenges in a legal perspective. *Comparative Policing from a Legal Perspect*. 2018;p. 228–54.


Author biography


Gurleen Kaur, Assistant Professor  <https://orcid.org/0009-0000-3652-0962>

Debhjit Mukherjee, PG Student  <https://orcid.org/0009-0009-5673-2554>

Bhavika Moza, PG Student  <https://orcid.org/0009-0001-9019-6267>

Vaishali Pahwa, PG Student  <https://orcid.org/0009-0002-0266-7047>

Kulwinder Kaur, PG Student  <https://orcid.org/0009-0001-1848-7510>

Kamaljeet Kaur, PG Student  <https://orcid.org/0009-0004-2579-0755>

Cite this article: Kaur G, Mukherjee D, Moza B, Pahwa V, Kaur K, Kaur K. The dark web: A hidden menace or a tool for privacy protection . *IP Int J Forensic Med Toxicol Sci* 2023;8(4):160-167.