Dark Web: Ethical and Legal Framework, Risks, Strategies

The dark web is a deep sea that harbors many dangers. When diving into this sea, it is vital to be sensitive to safety precautions and to act consciously. In this diving adventure, you are faced with a wide range of legal and illegal content. For this reason, you need to act in accordance with ethical principles and know what you are doing. In this report, I will talk about the risks you face, the precautions that can be taken against these risks, the legal framework regarding the crimes on the dark web, and the ethical issues that must be respected while swimming in this sea.

Let's start by talking about the risks. The dark web is basically a structure built on anonymity. This anonymity especially attracts and attracts malicious people who carry out illegal activities. Of course, the Dark Web attracts the attention of security forces as well as malicious people. A considerable part of the dark web is full of deceptive content such as fake content, phishing and fraud. Here, malicious people aim to harm people by luring them into their networks, while security forces are busy hunting down potential criminals. Another risk factor is terrorist groups. While surfing the dark web, you can be targeted by terrorist groups and find yourself in the middle of their activities. You can also become a target of various underground organizations and become their victim. You can also become a victim of hackers, or you can become a potential criminal in the eyes of security forces and face legal proceedings. Finally, the dark web carries many risks that have the potential to irrevocably ruin your life or the lives of others.

So what precautions can we take against these risks? Let's explain this step by step. First, you should take security measures on your device before connecting to the dark web. Here are some things you can do in this regard:

1) Connecting to the dark web through a virtual machine and protecting it from direct connection to your main network.

2) Use disk encryption.

3) Use a strong and reliable firewall.

4) Use reliable antivirus programs.

5) Use up-to-date versions of the operating system and applications.

The second step is to adjust browser settings. In this step, careful adjustments should be made on issues such as cookie clearing, tracking blockers, permitted authorizations, and a reliable and up-to-date browser should be used.

The third step is to ensure network security. Here are the things you can do in this regard:

1) Instead of connecting directly to the network adapter on the system, create and use a virtual network adapter on a virtual machine using a reliable gateway solution.

2) Hiding your IP address using network technologies such as Tor, I2P, etc.

In the fourth step, we are now connected to the dark web and there are a number of considerations and precautions to take. These are mainly the following:

1) Be wary of deceptive content and question its credibility.

2) Be very careful about clicking on links.

3) When creating any membership, use emails from secure services such as ProtonMail and do not use these emails for your daily use or private business.

4) When setting passwords, use strong passwords from trusted password management applications and keep these passwords in an encrypted database.

5) Be very careful when communicating with anyone and make sure that you do not reveal any information about yourself in communication.

6) Use services that use trusted anonymity technologies for file sharing.

7) Use reliable communication systems that provide anonymity and encryption for communication.

8) Refrain from illegal activities.

9) Not to use even the slightest information about you in any way, anywhere.

10) Disguise yourself with various fake identities, avoiding using the same fake identity all the time.

Now that we know the risks and the precautions that can be taken, we can draw a general legal framework for the crimes found on the dark web. While the legal processes differ in each country, the main framework is similar for a certain part of the world. In this report, I will describe the legal system in Turkey, but you can see similar frameworks in European countries, as the legal regulations on these issues in the Turkish legal system are based on European Union directives.

Turkish Penal Code (TCK): The Turkish Penal Code defines various crimes and sets criminal sanctions. Dark web activities such as hacking, breach of personal data, use of stolen credit cards are also covered by the Turkish Penal Code. Depending on the seriousness of the offenses and the amount committed, fines or imprisonment may be prescribed.

Information and Communication Technologies Authority (ICTA) Regulations: The ICTA publishes regulations on internet crimes and other digital issues. These regulations are important for regulating internet use and combating crimes in Turkey. For example, there are rules set by the ICTA on issues such as the protection of personal data and the regulation of online commerce.

Law on Debit and Credit Cards: Turkey has specific legal regulations on the issuance and use of debit and credit cards. Crimes such as the use of stolen credit cards are regulated under this law and criminal sanctions are determined.

Personal Data Protection Law (KVKK): The LPPD contains legal regulations to prevent the processing, protection and misuse of personal data. Crimes such as data breaches on the dark web and misuse of personal data are also covered under this law and criminal sanctions may be imposed.

International Cooperation Agreements: Turkey has entered into international cooperation agreements with other countries. These agreements provide for cooperation on issues such as extradition, evidence and information sharing. In relation to crimes on the dark web, international cooperation is important and Turkey acts within the framework of these agreements.

In the last part of our report, we will talk about ethical considerations. Ethical behavior on the dark web is actually difficult and the risk of unethical behavior is high. Therefore, utmost care is essential in order to act in an ethical manner. Here are some of the ethical rules to follow when surfing the dark web:

1) Any illegal activity should be strictly avoided, and if the intention is to observe such activities, passive observation should be made without involvement.

2) Respect the confidentiality of identity information.

3) If information is collected for the purpose of sharing information, pay attention to the information provided by the other person and obtain their consent by clearly stating that you will share information.

4) Investigate the accuracy of the information obtained.

5) Be aware of and avoid racist, unethical and toxic content.

6) If you are conducting research, obtain the necessary authorization from the appropriate authorities and follow certain ethical guidelines.

GitHub Repository: https://github.com/umutsertkaya/CTI_Project_Team_My_Progress