Types of cyber-enabled crime and their criminalisation

Oerlemans, J.; Hingh, A.E. de; Wagen, W. van der; Weulen Kranenbarg, M.

4 Types of cyber-enabled crime and their criminalisation

Jan-Jaap Oerlemans, Anne de Hingh & Wytske van der Wagen*

4.1 Introduction

In this chapter, we focus on cyber-enabled crime. Cyber-enabled refers to crime where computers and the internet are used as tools to commit traditional crime (Tollenaar et al., 2019; Wall, 2014; see also Chapter 1). We will take a closer look at the most common types of cyber-enabled crime, namely online criminal marketplaces, money laundering with virtual currency, online fraud, online sexual offences and online expression offences.

In cyber-enabled crime the internet often serves as a setting, for example to target victims or to distribute illegal goods, services or content. For a proper understanding of cyber-enabled crime, we first explain the difference between the clear web, the deep web, and the dark web. We then discuss the most significant types of cyber-enabled crime and their criminalisation. Finally, we highlight several future developments and present study questions and key concepts related to cyber-enabled crime.

4.2 The clear, the deep and the dark web

Within the infrastructure of the internet, three layers can be distinguished. The clear web – also called the 'public web' or 'surface web' – is the directly accessible part of the internet, such as the indexed websites that can be found via Google's search engine using a standard web browser.[1] The 'deep web' is that part of the internet that is not directly accessible and not indexed

* Prof. Dr. J.J. Oerlemans is assistant professor in Criminal Law at the Institute of Criminal Law & Criminology at Leiden University and endowed professor of Intelligence and Law at Utrecht University. Dr. A.E. de Hingh is an assistant professor in Internet Law at VU University Amsterdam. Dr. W. van der Wagen is a criminologist specialised in cybercrime.

1 A. Greenberg, 'Hacker Lexicon: What Is the Dark Web?', *Wired.com*, 19 November 2014.

by search engines, and may require logging in first or can only be accessed through a specific URL. Content on the deep web could include webmail, private profiles on social media services, or a scientific article behind a publisher's payment wall. The 'dark web' is that part of the internet that can only be accessed via a particular protocol and where the IP addresses of connected computers are hidden.[2] This three-tiered classification of the internet is often presented in the form of an iceberg (see figure 4.1).

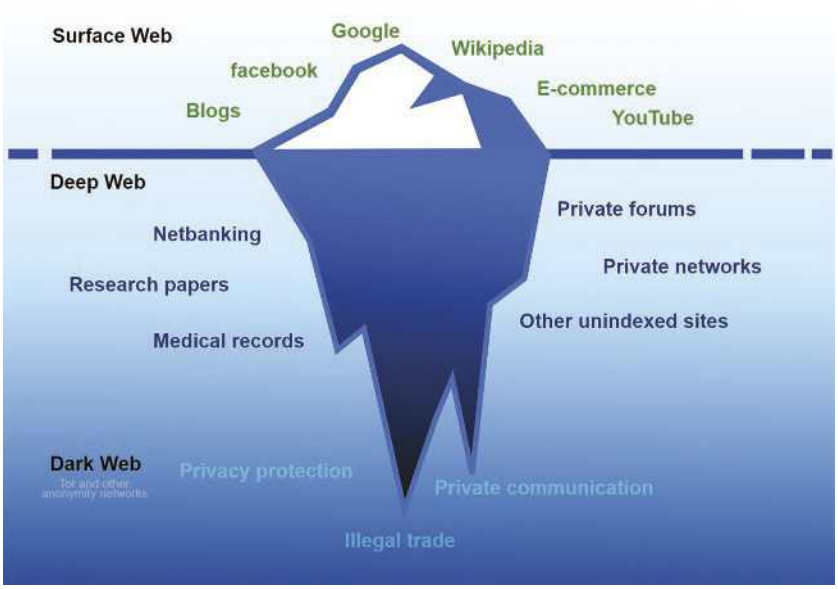

Figure 4.1 Visualisation of the distinction between the clear web, deep web and dark web[3]

Finally, a 'darknet' is a network of computers communicating via a certain protocol with hidden IP addresses. It is possible to visit websites on the dark web via a darknet. In other words, a darknet is the infrastructure that makes the existence of the dark web possible. The best-known system for connecting to a darknet is 'The Onion Router' (Tor). Tor, as a web browser, can be downloaded and installed by anyone. The operation of Tor was first explained in a paper by Dingledine, Mathewson and Syverson (2004). The Tor system sends internet traffic past (at least three) servers and encrypts network traffic in the meantime. The intermediate Tor servers do not record any data and

2 See, for example, A. Greenberg, 'Hacker Lexicon: What Is the Dark Web?', *Wired.com*, 19 November 2014.

3 Source: Ranjithsiji, 'Iceberg of Webs', Wikipedia.org, 17 April 2018.

only the IP address of the last Tor server (also called 'Tor exit node' or 'Tor exit relay') is visible. Figure 4.2 visualises an internet connection via the Tor system from a home with broadband internet.

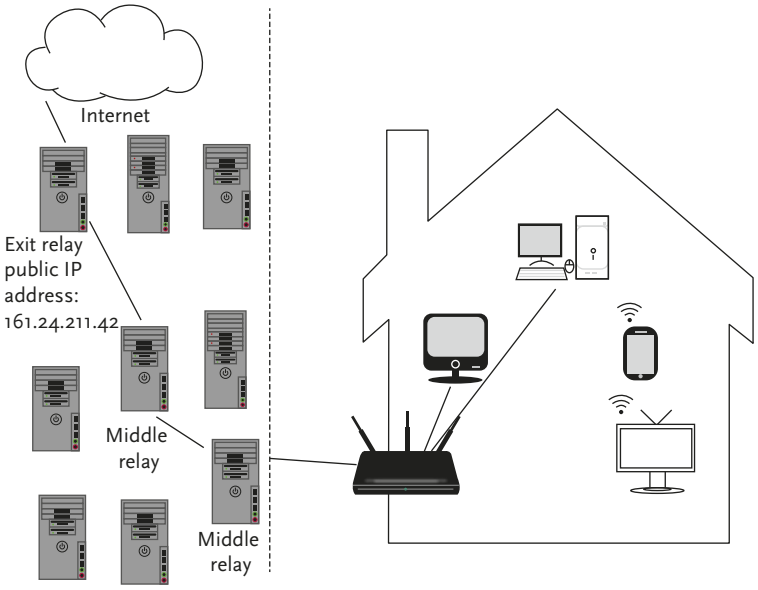

Figure 4.2 Visualisation of a Tor connection from a home[4]

Besides the benefits of (more) anonymity by disguising the original IP address of the computers connecting through the system and by encrypted internet traffic, the Tor system also allows accessing certain services that are not on the clear web and deep web. The services that can only be accessed via a darknet, such as Tor, are called 'hidden services'.[5] These can include websites, forums, chat services and email services.

The anonymity that the Tor system offers internet users makes it attractive to criminals. At the same time, Tor is also used for internet users who simply want to have more privacy and use the internet more anonymously. This includes journalists who want to protect their sources and communicate securely or people living in dictatorial regimes who would also like to read

4 Source: Oerlemans, 2017a, p. 41.

5 Besides Tor, there are other programs that can be used to access darknets, such as I2P and Freenet.

uncensored news sources or communicate with like-minded people (Gehl, 2018).

4.3 Online criminal marketplaces

Online marketplaces are digital environments or platforms where supply and demand come together. Within the context of this book, we specifically focus on marketplaces that trade in illicit goods (such as drugs and weapons), services (such as hacking tools) or data (of victims). Online criminal marketplaces are quite similar in function to a legitimate shopping mall in the physical world or web shops on the internet (Copeland et al., 2020; Odabaş et al., 2017; Smirnova & Holt, 2017) and, as we will explain, can be found both on the clear web and the dark web.

Online criminal marketplaces on the clear web and dark web are often structured similarly to internet forums. They use specialised software which displays conversations in a certain order and are structured around topics in so-called subforums. Within these subforums, individuals can start a 'thread' by posting a message with a question or an offer to buy or sell a particular product. In the context of online marketplaces where goods or services are sold, vendors usually maintain their own threads in which they can update products they advertise. Vendors post detailed information here about the payment process, means of communication and the delivery of goods. They can also explain how to get a refund or exchange products in case of faulty goods or services. Customers can then also leave ratings or feedback on the quality of the goods or services provided (Dupont et al., 2017; Holt, 2013a; 2013b; Holt & Lampke, 2010; Madarie et al., 2023).

Internet forums and online marketplaces are also called 'cybercriminal convergence settings' (Leukfeldt et al., 2017; Roks & Monshouwer, 2020; Soudijn & Zegers, 2012). Typically, three functions are distinguished in online marketplaces: 1) the market function; 2) the social function; and 3) the learning function. The market function involves the trade of illegal goods and data, the social function is about using platforms to connect and interact with other potential offenders, and the learning function is about exchanging information and knowledge between participants (Leukfeldt et al., 2017). They are stable and predictable place where cybercriminals gather, providing structure and continuity to its users , not unlike physical meeting places in cafés, parks and 'safe houses'(Felson, 2003, see also Chapter 6).

In addition to online marketplaces, 'single vendor shops' are common. Here, vendors can sell specific products directly to customers without the direct competition that exists in forums and crypto markets (Décary-Hétu et al., 2016; Smirnova & Holt, 2017). These sites use common e-commerce tools and platforms to efficiently engage with customers and distribute goods (Hutchings & Clayton, 2016; Martin, 2014; Smirnova & Holt, 2017). Moreover, vendors can link advertisements on forums and online marketplaces to their own shops to better market their products in the cybercriminal marketplace (Ablon et al., 2014; Martin, 2014; Smirnova & Holt, 2017).

In this chapter, we further focus only on online marketplaces. In what follows, the following types of online marketplaces and their criminalisation are discussed: marketplaces on the clear web, marketplaces on the dark web ('darknet markets') and marketplaces on communication apps.

4.3.1 Criminal marketplaces on the clear web

We often think that all criminal online marketplaces exist on the dark web, but this is not the case. Websites on the surface web can also function as (fake) web shops offering illegal goods, such as drugs and weapons, illegal services (such as tickets for concerts or zoos, money laundering services, or access to hacked computers), and stolen data (e.g. credit card or personal data).

For example, when it comes to drug trafficking on the clear web, the Dutch Trimbos Institute (a research and policy institute on substance abuse) distinguishes two types of illegal online marketplaces, namely (1) webshops that offer illegal drugs and (2) webshops that sell psychoactive drugs, which are often derived from already illegal drugs, but are not yet formally listed as illegal drugs (Olijhoek et al., 2021). Some online marketplaces present themselves as online 'pharmacies', where drugs such as cocaine or XTC can be ordered (see also Barratt & Aldridge, 2016; van Beek et al., 2023).

Case study: Farmer's Market

The Farmer's Market, formerly known as 'Adamflowers', is an early example of an online market for illegal drugs. It was founded in or before 2006 and was first active on the clear web. It was closed in April 2012 after the arrest of several vendors and buyers as a result of 'Operation Adam Bomb', i.e. a two-year investigation led by the U.S. Drug Enforcement Administration (DEA) in cooperation with law enforcement authorities in the Netherlands, Colombia, and Scotland. To enable a degree of anonymity, users made use of nicknames and the email service Hushmail, an encrypted email service promoted as private and anonymous.[6] It then moved to a hidden site on Tor in 2010, and expanded its services with new customer service features.

Ttech-website Ars Technica described Farmer's Market 'like an Amazon for consumers of controlled substances'.[7] The market allowed for several payment methods, including cash, PayPal and Western Union. The site sold drugs such as LSD, MDMA, mescaline, fentanyl, ketamine, DMT, hashish, psilocybin, and marijuana.[8] According to the DEA, Farmer's Market processed about $1 million between 2007 and 2009, and in 2011 the owners made $261,000 through PayPal alone. By 2012, about $2.5 million transferred through the site in total.[9]

A Dutch national pleaded guilty to drug trafficking and money laundering charges, admitting that he was one of the leaders of Farmer's Market. He was sentenced to a 12-year prison sentence in 2014. In 2016, he was transferred back to the Netherlands to serve his sentence, under an agreement reached with the U.S. authorities. Judges in the Court of Utrecht reduced the sentence to 6,5 years, given the time

6 J.M. Schwartz, 'Feds Bust "Farmer's Market" for Online Drugs', *Dark Reading*, 17 April 2012.

7 D. Goodin, 'Feds shutter online narcotics store that used TOR to hide its tracks', *Ars Technica*, 16 April 2012.

8 See, e.g., K. Zetter, '8 Suspects Arrested in Online Drug Market Sting', *Wired.com*, 16 April 2014.

9 V. Kim, 'Dutch national pleads guilty to running online marketplace for drugs', *Los Angeles Times*, 3 September 2014.

he had already spent in prison and time off for good behaviour. He was released the same year.[10]

Case study: RaidForums

RaidForums is another example of an online marketplace on the clear web on which illegal data was distributed.[11] This internet forum distributed hacked and copied data, hacking tools and pornographic material between 2015 and 2022. It was founded by a Portuguese national, using the nickname 'Omnipotent'. He was arrested in 2022.[12] The forum operated using a system of 'credits' that allowed members to access privileged parts of the website and 'unlock' and download compromised databases. Members could also earn credits in other ways, such as by posting instructions on how to perform certain illegal acts.[13]

People could easily log on to the forum and subpages, such as 'Leaks Market', and thereby access the material offered on the online market. For example, data of 700 million LinkedIn users were offered on RaidForums.[14] In total, more than 10 billion files were offered and the forum had more than half a million members.[15] The website was made inaccessible by the FBI and other police forces on 12 April 2022, during

10 DutchNews.nl, 'Online drugs dealer has US jail term cut by Dutch judges', 22 June 2016.

11 The word 'raid' in RaidForums is a reference to the forum's beginnings in 2015, when it was primarily an online place for organising and supporting various types of online harassment, such as sending the police to an address of an unsuspecting innocent person.

12 Indictment of 30 August 2022 of the United States District Court of the Eastern District of Virginia.

13 United States Attorney's Office, 'U.S. Leads Seizure of One of the World's Largest Hacker Forums and Arrests Administrator', 12 April 2022.

14 L. Mathews, 'Details On 700 Million LinkedIn Users For Sale On Notorious Hacking Forum', 29 June 2021, *Forbes.com*.

15 Europol, 'One of the world's biggest hacker forums taken down', Europol.europe.eu, 12 April 2022.

which the web servers were seized. Authorities may have been able to watch transactions taking place on the forum for some time.[16]

In 2023, three suspects were arrested in the Netherlands.[17] The website had thousands of Dutch users. In cases such as these, it is policy of Dutch law enforcement authorities that, depending on the activity on such a forum, users receive an email or a letter from the police informing them that they are users of an illegal online market and that the police took down the website. It contains an emphatic call to stop the illegal activities and a warning regarding the consequences of these crimes. Minors also received a cease-and-desist notice from the police.[18]

4.3.2 Darknet markets

Many criminal marketplaces are located on the dark web. These are called 'darknet markets' or 'cryptomarkets'. The name 'darknet market' reflects that it can only be accessed through a darknet, such as the Tor system, whereas the name 'crypto market' expresses that payments are made via so-called cryptocurrencies such as bitcoin or monero (Barratt, 2012; Martin, 2014; see also Section 4.4). Another typical feature of these markets is that delivery of the product is done by (postal) mail (Verburgh et al., 2018).

16 S. Lyngaas, 'FBI and international partners seize control of popular hacking forum', *CNN.com*, 12 April 2022,.

17 See also Court of Amsterdam 19 June 2023, ECLI:NL:RBAMS:2023:3748.

18 Politie.nl, 'Politie benadert afnemers gestolen data' ['Police approach buyers for stolen data'], 12 April 2023, *Politie.nl*.

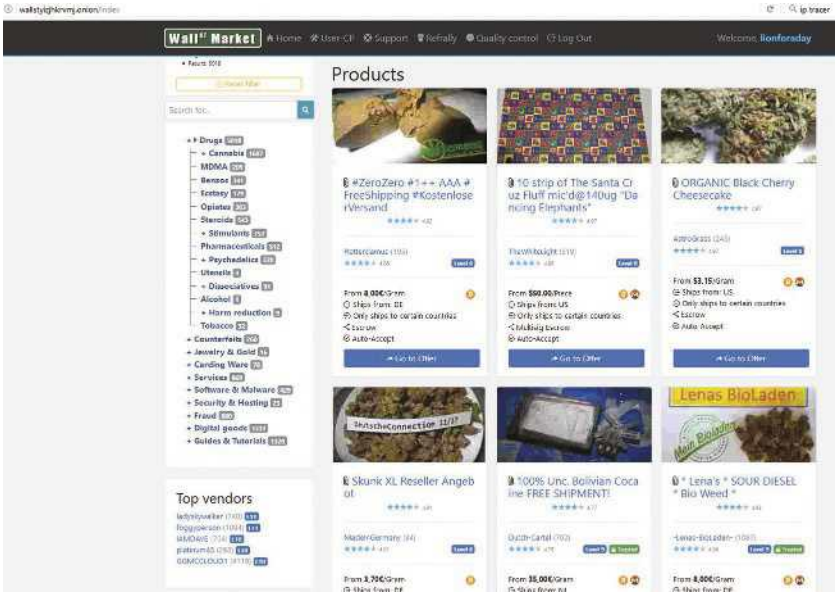

Figure 4.3 Screenshot of the darknet market 'Wall Street Market'[19]

A wide variety of illegal products and services are traded on darknet markets. From drugs and weapons to cybercriminal tools and stolen data (see, among others, Broadhurst et al., 2018; Broadhurst et al., 2021; Holt & Lampke, 2010; Holt & Lee, 2022; Martin, 2014; Ouellet et al., 2022; Soska & Christin, 2015; van Wegberg et al., 2018). With regard to arms trade, for example, it involves a multifaceted range of weapons, from simple pistols to sophisticated military weapons (Holt & Lee, 2023), but also tasers, knives, explosives and ammunition (Broadhurst et al., 2021). It is worth mentioning that weapons on these online marketplaces are many times more expensive than through the clear web or through official offline outlets in the U.S. (Holt & Lee, 2023).

On darknet markets (as well as on internet forums), there is often a strict hierarchy among users. Different tasks and responsibilities are distributed in order to try to maintain order and remove undesirable members or troublemakers. 'Administrators' set the rules, purpose and direction of the forum or marketplace. 'Moderators' often oversee the forum and change or modify the content on the site. These people are often experts in a particular field and are trusted by the administrator. Vendors, as mentioned earlier, can often gain a certain status through good ratings ('reviews') from customers

19 Source: archive of J.J. Oerlemans.

('buyers'). The quality of their products and the delivery process is therefore constantly assessed (Holt, 2012). Customers base their decision to use the services offered on it (Szgeti et al., 2023). The importance of reviews is evident, for example, in the following quote from a gun seller on the dark web (Holt & Lee, 2023, p. 523-524).

> It's really important to leave a review after purchase. Reviews can only be left by 'verified owners'. We already sold a lot of products [on this cryptomarket] but no one left a review of the purchased product, despite the fact that users are satisfied with the purchased products and are happy to come back for more. So please leave review and let know everyone else about your opinion. It is also important for me and other people who work hard on this shop to make our service better. We want to be sure that our products will have appropriate descriptions and an adequate price for the value of the file. Anyone who leaves reviews under the purchased product will receive a discount code for subsequent purchases entitling to a 40% discount.

The revenue model of darknet markets is usually as follows. For every transaction between a buyer and seller, the operator of the online market receives a small percentage in cryptocurrency. The darknet market also often facilitates the transaction by acting as a third party to hold the funds until the buyer gives the green light and payment can pass to the seller (this is called an 'escrow' system).

Estimates of how successful these darknet marketplaces are and the profits they amass vary enormously. According to the United Nations Office on Drugs and Crime (UNODC, 2023), the turnover of darknet markets had grown from hundreds of millions of dollars in 2016 to $2.1 billion in 2021. For trade in stolen data, according to Howell et al. (2023), who analysed thirty different darknet markets, it is also estimated to be several millions on average. Estimates regarding arms trade via the darkweb are at 960,000 per year (Holt & Lee, 2023). Darknet markets experienced a rapid growth until 2022, with a huge spike in the sale of drugs, weapons and hacking tools on the dark web in 2021 (Décary-Hétu & Giommoni, 2017; UNODC, 2023).[20]

20 Since 2022, police operations have reduced the size of the market, making it more difficult to monitor these markets and make estimates of revenue, according to UNODC.

Case study: Silk Road

'Silk Road' was one of the largest and most modern online drug trafficking sites on the internet from 2011 to 2013 and operated in the manner described above.[21] All transactions were conducted with bitcoin and the goods (mostly drugs) were delivered via postal mail. Silk Road also made use of an automated escrow payment system and automated review system.

In the case of Silk Road, the administrator – with the nickname 'Dread Pirate Roberts' – was found to have $28 million worth in bitcoin stored in his digital wallet after two years of work when he was arrested. The money was eventually sold through an auction.[22] Ross Ulbricht was indicted on charges of engaging in a criminal organisation, drug trafficking, and four conspiracy charges related to drug trafficking, computer hacking, money laundering, and false identity documents.[23] On 29 May 2015, Ulbricht was given the sentence of life imprisonment without the possibility of parole.[24] He was denied appeal.

The story of Silk Road gives an insight into the scale and level of professionalism of drug trafficking via the dark web. After Silk Road, many other darknet markets followed on the dark web. Examples of other darknet markets include Silk Road 2.0 (2014), Evolution (2015), AlphaBay (2017), Hansa (2017), DreamMarket (2019) and Hydra (2022) (Goonetilleke et al., 2023; Maras et al., 2023; van Wegberg & Verburgh, 2018). Many of these online drug marketplaces have since been taken offline by police operations. Some darknet markets also suddenly stopped . The administrators then took the funds held in escrow with them (a so-called 'exit scam').[25]

21 See extensively J. Bearman, 'The Rise and Fall of Silk Road', *Wired Magazine,* 23 May 2015.

22 U.S. Department of Justice, 'Manhattan U.S. Attorney Announces Forfeiture Of $28 Million Worth Of Bitcoins Belonging To Silk Road', 16 January 2014.

23 U.S. Department of Justice, 'Manhattan U.S. Attorney Announces The Indictment Of Ross Ulbricht, The Creator And Owner Of The "Silk Road" Website, 13 May 2015.

24 Sam Thielman, 'Silk Road operator Ross Ulbricht sentenced to life in prison', *The Guardian*, 29 May 2015.

25 See, for example: Andy Greenberg, 'The Dark Web's Top Drug Market, Evolution, Just Vanished', *Wired.com,* 18 March 2015.

In the context of this debate, the Dutch Trimbos Institute (mentioned earlier), uniquely underscored the potential drawbacks of shutting down online marketplaces in 2017. It argued at the time that buying drugs through the internet is safer for users than buying drugs on the streets. Moreover, the rating and payment systems used by online marketplaces give consumers more guarantees about the quality of the goods and delivery methods.[26]

4.3.3 Marketplaces on communication apps

As already explained, it is necessary to use a darknet such as Tor to connect to a (hidden) web server of an online market on the dark web (a darknet market). The fact that this requires some technical competence raises barriers to purchasing drugs, making it more likely for users to opt for social media services and communication apps (Barratt & Aldridge, 2016; van Beek et al., 2023). This brings us to the increasing trade of goods and services through social media platforms and communication apps (Demant et al., 2019; Moyle et al., 2019; Salinas, 2018; Søgaard, 2019).

Social media services are also used to communicate between people about the purchase of narcotics, for example, but it is also a platform on which, depending on technical functionalities, commercial dealers can offer their products and services to reach new potential customers (Moyle et al., 2019). Literature also points to drug markets on popular services, such as Snapchat, Instagram and Facebook (Bakken & Demant, 2019; Bakken, 2020; Demant et al., 2019; Moyle et al., 2019; UNODC, 2023). However, there is increasing empirical evidence that in such places there is also a lively trade in tools and services related to cybercrime, and particularly all kinds of fraud (see, among others, Bekkers & Leukfeldt, 2022; Bekkers et al., 2023). The scale of these types of markets and how much profit is generated is not yet known.

Research shows that communication apps such as Whatsapp, and especially Telegram, are used to trade illegal services, goods and data, and are also used for sexual offences, fraud and scams (van Beek et al., 2023; Garkava

26 M. Hijink & L. van Lonkuyzen, 'Platleggen drugshandel op internet werkt averechts' ['Taking down online market places is counterproductive'], *NRC.nl*, 28 August 2017.

et al., 2024; Roks & Monshouwer, 2020).[27] Telegram Messenger is a free messaging service that allows users to share encrypted messages, photos and video files that can also be assigned a self-destruct function (Moyle et al., 2019). In addition, users have the option to communicate more anonymously using end-to-end encryption in the so-called 'Secret Chats'. This feature is typically used when buyers are interested (Garkava et al., 2024). Due to these functionalities, Telegram presents itself as a secure messaging service that is also more accessible in terms of access and use than, for example, darknet markets (Roks & Monshouwer, 2020; Roks & Hendriksen, 2021).

When people start trading in a group app or channel (such as on Telegram), an online market is created. Channel administrators play an important role in this. They determine who gets access to the group, set the rules and penalties and monitor them (Dewey & Buzetti, 2024). An important difference between communication apps and darknet markets, is that communication apps allow direct contact and quick delivery of the good (e.g. drugs) (Childs et al., 2020). In addition, as mentioned earlier, it is easier to purchase drugs through a communication app than on the dark web, as the latter requires some technical expertise (Moyle et al., 2019). Garkava et al. (2024) also point to similarities in types of online marketplaces, such as the preferred use of cryptocurrencies, rules on what is allowed and prohibited on these marketplaces, the availability of manuals and explanations and the use of escrow services for the transactions (see also Hutching & Holt, 2015). Garkava et al. (2024) suspect that it is more difficult for Telegram users to assess whether a group or channel on Telegram is trustworthy, due to its different structure and the lack of a review system.

The Trimbos Institute, for example, found in 2023 that WhatsApp is most frequently used to get drugs by young adults in the Netherlands. One difference with WhatsApp is that Telegram facilitates larger trading volumes and offers the possibility to search by keywords and region (van Beek et al., 2023). Finally, research shows that combinations of platforms are also used when purchasing drugs, such as sharing links to web shops on the clear web as well as the dark web (van Beek et al., 2023).

27 I. de Zwaan, 'Telegram is het nieuwe darkweb voor kinderporno: "Zelfs onze rechercheurs werden stil van de beelden"' ['Telegram is the new darkweb for child pornography: "Even our detectives became quiet on seeing these images"], *Volkskrant.nl*, 5 April 2024.

4.3.4 Criminalisation

Regarding the criminalisation of illegal trade on online marketplaces, there are not many surprises. Trade in illegal goods, such as drugs and weapons, are criminalised in most countries in criminal laws.

It does not matter whether the illegal trade takes place on the clear web, the dark web, in a channel on Telegram or on the streets. Since there are no specific provisions specifically addressing online drug trafficking in the Convention on Cybercrime, we will not go in further detail.

Case study: illegal trade on RaidForums

On 3 November 2023, the Court of Amsterdam convicted a Dutch hacker for computer hacking, extortion, fencing non-public data, ransomware, and money laundering in excess of one million euros.[28]

In this case, the accused had in his possession stolen databases containing data of 7,3 million people, which he himself had obtained through hacking. This included personal data of hundreds of thousands of Dutch people who had bought tickets for an amusement park, zoo, event or museum through a company called Ticketcounter. Data of 1,5 million ticket buyers, including dates of birth, addresses, phone numbers and bank account numbers were offered by the hacker on RaidForums.[29] Furthermore, the data of a health care organisation and an internet forum for prostitution clients also fell victim to extortion.[30]

The accused was given a prison sentence of four years (one year conditional). This case shows that these illegal behaviours can be categorised as both cyber-dependent crimes and cyber-enabled crime.

28 See Court of Amsterdam 3 November 2023, ECLI:NL:RBAMS:2023:6967.

29 S. Hulsen, 'Hoe Ticketcounter-directeur Sjoerd na datadiefstal appte met een crimineel' ['How Ticketcounter director Sjoerd communicated with a criminal after data theft'], *RTL News*, 23 February 2023.

30 'OM eist zes jaar tegen Zandvoorter voor grootschalige datadiefstal: "Unieke zaak, qua aard en omvang"' ['Public Prosecution Service demands six years against Zandvoorter for large-scale data theft: "Unique case, both in nature and scale"'], *AD.nl*, 22 October 2023.

4.4 Money laundering with virtual currency

Virtual currencies, such as bitcoin and monero, are often used to buy illicit goods and services and to launder money. Virtual currencies are based on cryptographic software involving no central authority to oversee the management of the money (e.g. Oerlemans et al., 2016). It is important to note that virtual currencies (also called 'cryptocurrencies') are not officially recognised as 'real money' (fiduciary currencies, such as euros and dollars) or digital money (in a bank account). From a legal perspective, virtual currencies are therefore merely bits and bytes to which value is assigned by individuals.[31]

Bitcoin transactions work as follows. During a bitcoin transaction, a network of bitcoin users verifies together whether a transaction is legitimate or not. The network acts as a kind of registry and that registry is also known as the 'blockchain'. Bitcoins are sent to a bitcoin address, such as '1X6GYUigC9tYGqdNPJyL2769U9jd8P3vT', via a website or via apps connected to the blockchain. Bitcoins are stored on a computer in a file, the so-called 'bitcoin wallet'. This digital wallet can be accessed via an internet user's account or, for example, on a USB stick. Through the digital wallet, it is also possible to transfer virtual currency to other wallets. All transactions in the blockchain are public and anyone who wants to can view and follow the transactions back in time. Bitcoins are therefore not anonymous, but it can be difficult to identify the individuals behind a bitcoin address. If a user's identity and bitcoin address become known, for example because the user of a certain bitcoin wallet with a bitcoin address himself reveals it on the internet, his entire transaction history can be traced.

Payments with cryptocurrencies can therefore be made easily, quickly, and all over the world without the intervention of regulated institutions (such as banks and other payment service providers).[32] The lack of supervision and relative anonymity are attractive to, for example, criminals who want to launder their illegally obtained assets.[33] The purpose of money laundering is to disguise the origin of money. In other words, to give illegal money a legal

31 Virtual currency is defined in Dutch anti-money laundering legislation as a 'digital representation of value', 'which is accepted as a medium of exchange', and 'can be transferred, stored and traded electronically'.

32 These transactions are not necessarily sufficient. For example, bitcoins produce a significant carbon footprint (Stoll et al., 2019).

33 Dutch Anti-Money Laundering Center (AMLC), 'What is money laundering with cryptocurrencies?', 30 August 2023.

origin.[34] Payments on darknet markets often take place in virtual currencies, such as bitcoin and monero (Barratt, 2012; Martin, 2014).

The relationship with cybercrime and virtual currency is also reflected in the use of ransomware, when the ransom is almost always transferred in cryptocurrency (Custers et al., 2020). As shown in Figure 4.4 below, in 2022, 20-billion-euro worth of global transactions were linked by the company ChainAlysis to crime in the following categories: CSAM, ransomware, stolen (crypto)money, funds directed to countries under sanctions (such as Russia and North Korea), money used to finance terrorism, scams (fraud), administrators of cybercriminal groups, fake web shops and darknet markets (UNODC, 2023).

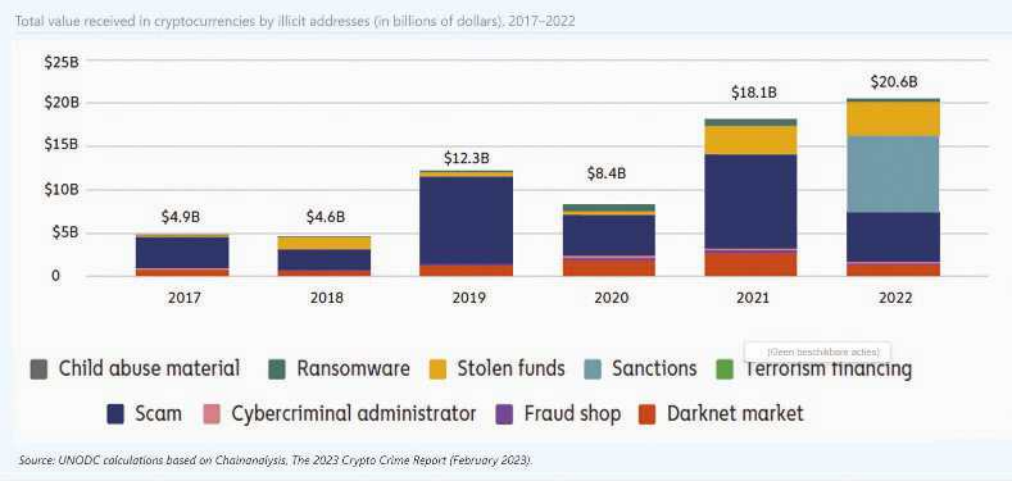

Figure 4.4 Total value received in cryptocurrencies by illicit addresses, 2017-2022

4.4.1 Regulation

The adoption of the fifth European Anti-Money Laundering Directive in 2018 was an important first step in combating money laundering through virtual currencies.[35] Certain crypto service providers are now regulated under the EU Directive. These include (1) *crypto-exchange platforms*, where one can exchange

34 See also Financial Intelligence Unit-Netherlands, 'What is money laundering?', *fiu-nederland.nl*.

35 EU Directive 2018/843 of 30 May 2018 amending Directive 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, OJ L 156.

virtual currency for other virtual currency (e.g. from bitcoin to monero or vice versa) or exchange virtual currency to fiat money (e.g. from bitcoin to the euro or vice versa); and (2) *crypto wallets* such providers of bitcoin wallets. These companies hold data that may provide important leads in money laundering investigations.

These companies also function as 'gatekeepers'. Therefore, they must take measures to prevent criminal offences such as money laundering and terrorist financing. The provider is therefore obliged to verify the identity of customers ('Know Your Customer' (KYC) policy) and must monitor for suspicious transactions. Unusual transactions must be reported to the 'Financial Intelligence Unit' (FIU).

Furthermore, a new EU regulation to counter money laundering with cryptocurrencies was adopted in 2023.[36] This regulation is broader than the fifth Anti-Money Laundering Directive and also covers other crypto services. It sets rules regarding consumer protection, countering market abuse and other requirements regarding the business operations of crypto-service providers. Many EU Member States are still in the process of implementing these EU anti-money laundering regulations.

4.4.2 Criminalisation

The criminalisation of money laundering with virtual currencies such as bitcoin is considered the same as money laundering with fiduciary (real) money. The criminalisation of money laundering behaviours often involves the possession or concealment of the illegal origins of money, or in this case virtual currencies. In many situations, money laundering of cybercriminal profits takes place in combination with 'traditional' money laundering methods. These methods can be straightforward or more complex. A typical example of a straightforward money laundering method is to create a (long) series of transactions, including several currency exchanges (including to and from cryptocurrencies such as bitcoin to monero to U.S. dollars), transfers to other countries and investments in real estate or other assets (such as expensive cars) (Custers et al., 2020). Typically, criminals split transactions to smaller amounts in order to avoid suspicion and transfer money via countries with less strict rules and supervision.

36 Regulation (EU) 2023/1114 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, OJ L150.

Another straightforward money laundering method is to spend the profits directly on products and services. An example of a more complex money laundering method are fictitious gambling profits. Although casinos are strictly regulated in many countries, online gambling is legal in many jurisdictions. By creating a number of online gambling accounts, criminals can transfer money between these accounts, concealing the origin of the profits (Custers et al., 2020).

With ransomware, criminals prefer payment in virtual currencies, because payments via online banking can easily be traced. Offenders often choose to first use so called 'mixing services'. These are online services that exchange bitcoins for bitcoins, against a fee. The obvious goal is to make using bitcoins more anonymous. After a user has submitted the bitcoins, the mixing service collects bitcoins from different sources and pays them back to the respective user on a different account (Miedema et al., 2023; Wegberg et al., 2018). When bitcoins arrive in an account of cyber offenders, they could exchange it to currencies such as euros or dollars. They can also choose exchanges that provide a degree of anonymity and no or minimal KYC policies or transfer the money to criminal online payment providers that offer to launder money (Custers et al., 2020).

In practice, many 'money laundering typologies' are distinguished that may be useful for proving money laundering with virtual currencies. Often times, countries have an Anti-Money Laundering Centre (AMLC) which publish these typologies on their website. Some of the above-mentioned modus operandi to launder virtual currencies are part of these typologies.

Case study: the laundering of bitcoins originating from Agora and Evolution Market

On 10 March 2017, a Dutch court convicted a defendant of online drug trafficking and money laundering.[37] The defendant was extensively involved in drugs trafficking, mainly XTC and LSD through the – at the time popular – darknet markets 'Agora' and 'Evolution'. The accused specialised in supplying so-called 'resellers' in larger quantities and thus belonged to the higher segment of the drug trade. The

37 Court of North Netherlands 10 March 2017, ECLI:NL:RBNHO:2017:1940.

evidence used, among other things, were the drug trafficker's reviews by customers on the forums.

The case details the virtual currencies used, in this case bitcoins, 'paycoins' and 'opalcoins'. The investigators checked whether a connection could be made between the bitcoin addresses in the digital wallet on the accused's laptop and the transactions and bitcoin addresses appearing on the darknet markets 'Agora' and 'Evolution Market'. They found that, during the period from 24 February to 9 March 2015, 889.90 bitcoins had been transferred to the forums with a value of €208,125.72.

The accused was convicted of money laundering. The origin of the cryptocurrencies (from online drug trafficking) was concealed by exchanging bitcoins into euros. These bitcoins originated from crime. The court qualifies the purchase of the luxury cars and luxury goods as acts of concealment, as they were purchased with money obtained with drug trafficking. The virtual money still in the defendant's possession and the luxury goods were forfeited by the court. Despite the relatively young age of the accused during the commission of these acts, the accused is sentenced to three years' imprisonment.

4.5 Online fraud

Online fraud is one of the most common types of cyber-enabled crime worldwide. According to the FBI, Americans approximately lost 10.8 billion dollars on a wide variety of online scams in 2022. Phishing was reported as the most common type of fraud.[38] In the same year, in the UK 73% of adults (40 million people) were targeted by fraud with a total loss of 19 million pounds. Less than a third of the victims reported the criminal offence to the police.[39] In 2023, of all types of cybercrime, Dutch people were most frequently a victim of scams and online fraud (9%), with purchase fraud

38 See L. Bar, 'Americans lost $10.8 billion to internet scams FBI says', *ABCnew.go.com*, 13 March 2023.

39 See '19 million lose money to scams, but fewer than a third report', *Nationaltradingstandards.uk/news*, 25 October 2023.

(from fake web shops) being the most common type of fraud (8%) (CBS, 2024).

Online fraud is often referred to as *phishing*: the angling (or 'fishing') for personal and/or confidential data such as usernames, passwords, IP addresses and bank details. Phishing can be described as a scam where data is collected from a person by tricking the target into providing personal or financial information. This is often done using an email or message that includes a link to a fake website (e.g. Loggen & Leukfeldt, 2022; van der Wagen & Bernaards, 2020). The obtained information is then sold to third parties or used to place orders over the internet using that data. Often times, phishing is untargeted; the same phishing message being sent all at once to a large group of victims. In case of 'spear phishing', on the other hand, persuasion techniques are tailored specifically to one victim.

Victims are often tricked into sharing personal or financial information through a website. Setting up a phishing website has become easy with the development of 'phishing kits'. This software acts as a tool to set up fake websites and can be bought, rented, or even downloaded for free on darknet markets, social media platforms or communication apps (such as Telegram). Often, the fraudulent website involves a fake online banking environment or fake online payment platform. The 'phished' data are often sent to an email address or collected in a 'phishing panel' (Bijmans et al., 2021).[40] Attacks on targets are often tailored to a particular audience and country. Although phishing attacks are often expected to become more technically sophisticated, the modus operandi has hardly changed over the years, according to Loggen & Leukfeldt (2022).

Case study: payment request fraud

In this case study, we take payment request fraud through Markplaats.nl as an example goods (Rooyakkers & Weulen Kranenbarg, 2020, p. 30-33). Markplaats.nl is a well-known Dutch online trading platform in second-hand. In this type of fraud, a seller is approached by a supposedly interested buyer (hereinafter: fraudster) using a hacked Marktplaats account through the Marktplaats chat option or by use of

40 See also Court of The Hague 1 July 2021, ECLI:NL:RBDHA:2021:6678 on phishing panels.

WhatsApp. For the fraudster, it is attractive to choose communication by use of WhatsApp, because the detection and warning systems of Marktplaats.nl do not work on that platform.

After contact, a brief negotiation takes place, after which agreement is reached on the sale (this often involves the fraudster offering the asking price immediately). Now that there is a deal, the fraudster sends an illegitimate payment request link to transfer one cent, supposedly to verify the seller's identity and convinces the victim to click on it. When this link is sent within the Marktplaats chat-environment, this takes place through a 'gateway link', or a forwarder-link to a phishing site. When contact is made through WhatsApp, the victim clicks on a URL and is redirected to a webpage that looks like a legitimate payment request, including associated logos and textual style. This phishing site has the 'look and feel' of a legitimate payment request.

On this online banking phishing site, personal data, such as username, password and debit card details, are then obtained by (supposedly) logging in to the online banking environment to complete the payment. In this way and by additional actions, the fraudster also captures authentication and verification codes in his panel. With this data, the fraudster logs into the victim's online banking account and linked devices (such as phones or tablets) owned by the fraudster to the victim's bank account. Without the victim's knowledge, the fraudster can now access the bank account and transfer money.

The last step (called 'cash out') is to transfer the money held in the victim's accounts, to which the fraudster now has access. Note that all components of this crime script (such as hacked Marktplaats-accounts and the phishing panel) and associated knowledge, can be purchased or hired over the internet for a low price (van Wegberg et al., 2018). Cash out is often done through transfers to money mules, who place online orders (credit cards, cryptocurrency or orders at online shops) or make payments in physical shops (from phones, through use of Apple Pay). Then, the fraudster (if contact was made through WhatsApp) will often delete the messages, preventing the victim from looking up the phone number or phishing URL sent.

Victims of payment request fraud are also often approached through WhatsApp or other communication apps by perpetrators. They use tricks, for example as in 'friend-in-need fraud'. This involves offenders posing as the victim's daughter or son, saying they have a new number. Soon they ask for money, for example because their bike or car has broken down and they do not have access to a debit card. Furthermore, 'CEO fraud' is an example of (spear) phishing. This involves abusing the identity of a company's chief executive officer (CEO) to instruct – usually via email – an employee in the finance department to make a payment (Europol, 2016; 2018). The message is tailored as much as possible to convince the victim to transfer money. In the Netherlands, for example, two directors of Pathé cinemas were scammed out of 19 million euro through a phishing mail.[41]

4.5.1 Criminalisation

Online scams are criminalised using the general offence for fraud. Fraud is often criminalised when someone uses a false name, capacity, or 'cunning tricks' to cheat someone out of goods or data. Note that, in many jurisdictions, merely failing to deliver a promised good or service offered on an online trading platform, does not automatically constitute a scam. To be recognised as a scam, it often requires adopting a false name or capacity, or employing cunning subterfuge. In principle, if a promised service or good is not delivered, citizens should claim their money back and follow civil proceedings.

When perpetrators impersonate another person, it may also constitute identity fraud. It is noteworthy that in phishing cases, offenders are often convicted for 'participating in a criminal organisation'. Given the common division of roles in committing cybercrime, this is quite conceivable. When malware is used to steal personal data entered on websites (e.g. by means of a 'keylogger'), this constitutes a computer crime as discussed in Chapter 3. If money is withdrawn from the victim's account or transferred by the offender to another account, this also constitutes the traditional crime of 'theft', using the acquired access data and/or bank card with its PIN code. When money mules or other acts of concealment are used, this may also constitute money laundering.

41 A ruling by the civil law sector of the Court of Amsterdam on the dismissal of one of the directors contains many details about the emails sent: Court of Amsterdam 31 October 2018, ECLI:NL:RBAMS:2018:7881.

4.6 Online sexual offences

The growing digitalisation in our lives has affected existing sex crimes and led to new (online) sex crimes. For example, the internet has made it much easier to distribute sexual images, such as child sexual abuse material, on a scale impossible in the physical world (Taylor & Quayle, 2006). The internet has also enabled the making of contact, anonymous or otherwise, over (long) distances, which has allowed for the emergence of crimes such as 'virtual sexual assault' or remote sexual assault (e.g. through extortion). This section examines sexual crimes in which the internet and IT play an essential role or serve as the environment in which these types of cyber-enabled crimes take place.

4.6.1 Images of sexual abuse of minors

In the creation or dissemination of child sexual abuse material (CSAM), computers and the internet already played a key role for decades. The rise of the internet in the 1990s created a global spread and growing online availability of CSAM. It was made available on websites, online forums and peer-to-peer sharing services. This growth is reflected, for example, in the massive amounts of material that suspects nowadays often have in their possession: case law regularly includes numbers such as hundreds of thousands and even millions of images of child sexual abuse (van den Hurk et al., 2023).[42]

Although the term 'child pornography' was a long-established term, nowadays the term 'child sexual abuse material', commonly abbreviated as CSAM, is preferred (van der Bruggen, 2023).[43] In simple terms, this type of cyber-enabled crime involves the creation or distribution of a photograph or a video of a child under the age of eighteen performing sexual acts, posing sexually or being present in a sexually oriented environment. In this book, we use the term 'child sexual abuse material' or the abbreviation CSAM.

42 See, for example, Court of Rotterdam 9 December 2009, ECLI:NL:RBROT:2009:BK6022, Court of The Hague 13 March 2013, ECLI:NL:RBDHA:2013:2872 and Court of Rotterdam 31 March 2017, ECLI:NL:RBROT:2017:2445, Court of Rotterdam 19 February 2024, ECLI:NL:RBROT:2024:1928

43 See also Defense for Children, 'Terminology guide on sexual abuse and sexual exploitation of children', 2022.

Societal attitudes towards the sexual material of minors have significantly changed and evolved over the years. For example, the 1960s was characterised as a time of relative openness and sexual freedom and expression, in which sexual contact between adults and minors was not rejected outright. At that time, people bought such material in sex shops or via mail order (Taylor & Quayle, 2003). From the 1980s onwards, a change in mentality took place. During that time, the women's movement emphasised the harmful effects of pornographic material, and it was pointed out by police and the judiciary that the production of pornographic material showing children was often accompanied by child abuse (Kool, 1999). Consequently, in the late 1980s, making and sharing images of sexual abuse of children under sixteen was criminalised in many countries. In 2002, the age limit of the victim was raised from sixteen to eighteen years, following the implementation of international treaties and EU regulations.

Over the years, a shift took place from physical meetings places to online forums or marketplaces (i.e. cybercriminal convergence settings), where persons interested in sexual materials of minors congregate. In her work, van der Bruggen explains how these images are exchanged on forums on the darkweb. On these forums, thousands to hundreds of thousands of individuals are deliberately seeking images of sexual abuse of minors and are willing to cross the line of what is legal (van der Bruggen, 2023). In contrast to other online markets like drug markets, this phenomenon does not revolve around financial gain. Instead, it involves some form of exchange or trading activity.

Online forums thus facilitate in the exchange of CSAM, but also in information related to that child sexual abuse (in so-called 'paedo(philic) handbooks') and the exchange of security tips to avoid detection by other people and law enforcement authorities. Members of these forums communicate with each other about certain topics, such as the type of material (e.g., 'boys versus girls', 'hardcore versus softcore', 'teen versus pre-teen'), informative sections (e.g. on techniques regarding computer security) and sections related to forum management where administrators welcome new members and explain the house rules (van der Bruggen, 2023). Sometimes higher-status members are given access to hidden parts of the forum if they submit material, which is often associated with a greater degree of prestige and authority.

Criminalisation

In most, if not all jurisdictions worldwide, sexual abuse of minors is criminalised (Schermer et al., 2019). Some states specially criminalise (a) sexual activities with minors that did not reach the legal age for sexual activities, (b) when offenders engage in sexual activities with a child where abuse is made of a recognised position of trust, authority or influence over the child (such as a school teacher, priest, or a position within a family), and (c) when a particularly vulnerable situation of the child is abused, notably because of a mental or physical disability or a situation of dependence.[44]

More specifically in relation to child abuse materials, Article 9 of the Convention on Cybercrime criminalises producing, offering, distributing, procuring, and possessing child pornography. The term 'child pornography' refers to child sexual materials that visually depicts: (a) a minor engaged in sexually explicit conduct; (b) a person appearing to be a minor engaged in sexually explicit conduct; (c) realistic images representing a minor engaged in sexually explicit conduct. Note that Article 9 does not explicitly criminalise 'accessing child pornography' through streaming videos made available on websites. Therefore, states may need to explicitly criminalise 'accessing' CSAM (e.g., Gercke, 2011).

States can decide themselves whether they set an age limit of eighteen or sixteen years (although a large majority of states sets it at eighteen) and states can decline criminalising the behaviours under points (b) and (c) which constitute 'virtual child pornography'.[45] In the Explanatory Memorandum to the Convention on Cybercrime virtual CSAM is further described as: images, which, although 'realistic', do not in fact involve a real child engaged in sexually explicit conduct. This includes pictures that are altered, such as morphed images of natural persons, or even generated entirely by the computer.[46]

The problem with virtual child pornography is that no physical abuse of a minor takes place during the production of the material. In the past, the rationale for criminalising CSAM was the damage inflicted at the time of the creation of the image and the protection of minors against the circulation of this material. The crime descriptions in most criminal law systems deal

44 See most notably, Art. 18 of the Lanzarote Convention. Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

45 Art. 9 Convention on Cybercrime.

46 Explanatory report of the Convention on Cybercrime, para. 101.

with real victims as opposed to 'virtual' victims. However, there are several reasons why criminal liability is also extended to virtual child pornography. These include avoiding evidentiary problems and the fact that the materials can be used to corrupt children (to 'groom' them for abuse), as well as the idea that virtual CSAM may act as a 'stepping stone' for consumers of child pornography, prompting them to move to real CSAM or even sexual abuse (Schermer et al., 2016, p. 28; Strikwerda, 2015). Some authors however point out that there is no scientific evidence that virtual images would encourage offenders to consume more CSAM or commit sexual offences involving minors. They also argue that the ban on virtual CSAM may negatively impact the possibilities of scientific research into the effects of the use of virtual CSAM as a treatment (Faassen et al., 2021). Despite those arguments, there is a trend in Europe to include virtual CSAM within the scope of prohibition of CSAM in general.

Case study: child sexual abuse material on a dark web forum

On 3 March 2020, a Dutch suspect was convicted for participating in a criminal organisation. Together with co-defendants, he was active on three online forums. The suspect himself functioned as 'chief administrator and hoster' of two chat rooms.[47] For example, he 'promoted' visitors to function of moderator if they stood out 'positively' for a longer period of time. The chat site staff had different ranks with their own chat channels. On those channels, people could talk more freely, because outsiders could not get in as easily. Members kept notes of meetings, which in retrospect contributed to evidence against users.

The Dutch court did not accept the defence's argument that sharing the text and links to sexual material of minors in the chat channels did not involve dissemination of child sexual abuse material. The warning on the chat channels that no CSAM should be distributed also did not convince the judges, because it could be inferred from other evidence that illegal material was distributed. In one of the chat rooms, 2,410 images were shared between 26 January and 14 June 2018, of which 298 involved child sexual abuse material.

47 See Court of Overijssel 3 March 2020, ECLI:NL:RBOVE:2020:913.

4.6.2 Sexting

The term sexting is a contraction of the words 'sex' and 'texting'. Nowadays, it refers not so much to textual content but to creating intimate or sexual images (e.g. with a camera or webcam) and sharing these images with another person by sending them to that other person using their mobile phone, computer or tablet (with mutual consent – this is also called primary sexting) (van Berlo & Ploem, 2018). When the images are forwarded to third parties after receipt, this is referred to as secondary sexting (Del Rey et al., 2019).[48] While sexting also takes place between adults, it is particularly common among adolescents and young adults. For adolescents sharing intimate, 'sexy' visual material is a normal and important part of their sexual development and discovery of one's own sexuality (Lievens, 2014; Witting 2019). Thus, the consequences of sexting certainly do not (always) have to be negative or harmful for those involved (Gorissen et al., 2020).

Criminalisation

Sexting is illegal when minors engage in making, possessing, or further distributing an image depicting sexual behaviour of themselves or the other person. This involves the manufacturing, possession, or distribution of 'a visual depiction with an unmistakable sexual intent' as referred to in Article 9 of the Convention on Cybercrime (the criminalisation of CSAM). Article 7 of the EU Directive on combating violence against women also criminalises 'the unsolicited sending, by means of IT, of an image, video or other similar material depicting genitals to a person, where such conduct is likely to cause serious psychological harm to that person'.[49] When adults engage in sexting, the act can also be criminalised when they use it for stalking (when the stalking is systematic and there is an unlawful and intentional infringement of a person's privacy) (ten Voorde, 2017).[50] In the EU Directive, the criminalisation is regarded as a type of 'cyber-harassment' (see also Section 4.7.2).

48 Notably, non-Dutch literature makes the distinction between primary and secondary sexting. See, for example: 'Sexting among young people: facts and figures', *Sensoa.be*, last accessed 12 April 2024.

49 Directive of the European Parliament and of the Council on combating violence against women and domestic violence, 25 April 2024, 2022/0066(COD).

50 See also Art. 6 of the EU Directive on combatting violence against women. Cyberstalking is as the intentional conduct of repeatedly or continuously placing a person under surveillance, without that person's consent or a legal authorisation to do so, by means of ICT, to track or monitor that person's movements and activities, where such conduct is likely to cause serious harm to that person.

As mentioned before, sexting is not always harmful for the sexual development of people. In the Netherlands, for example, the Public Prosecution Service does not prosecute for consensual sexting among minors. They will prosecute, however, when damage is caused to the depicted minor or when the images were created after deception or threats. For that reason, a distinction is made between three categories of sexting:[51]

- Category I: there are (indications of) commercial elements, pressure, coercion, deception, secret recordings, a dependency relationship, a victim younger than twelve years, a more than limited age difference (five years or more) or possibly other sexual offences; if the suspect is 23 years or older, this automatically constitutes Category I.
- Category II: there are indications of motives other than those in Category I; these include bullying, defamation, slander or intimidation.
- Category III: The visual material appears to be created voluntarily, the persons involved are both minors and there are no aggravating circumstances as described in Categories I and II.

In principle, the Dutch Public Prosecution Service also states that criminal law is not intended for offences that fall under Category III, because this is usually not legally possible or not in the interest of the parties involved to prosecute (Gorissen et al., 2020). Cases of Category I sexting are so serious that prosecution will usually be opted for. Category II sexting cases are also eligible for a conditional dismissal. In these cases, the choice is often made for the dismissal of the case of prosecution for libel or defamation (see Section 4.7).

4.6.3 Abuse of sexual imagery ('revenge porn')

The unwanted online publication of sexual images or videos of an ex-partner with the aim of antagonising that ex-partner has long been known as 'revenge porn'. Perpetrators of revenge porn are usually (i.e. not always) ex-partners who received sexually explicit images at the time of the relationship and spread them as revenge for the breakup of the relationship to publicly shame or humiliate the victim. However, revenge is not necessarily the (only) motive. Often the perpetrator wants to exert power over the victim, bullying, humiliating, insulting, or intimidating the victim. Research shows that factors such as strengthening friendships between perpetrators, regulating each other's sexual behaviour, or increasing one's own popularity also play a role in sexting (Gorissen et al., 2020). Thus, the term 'revenge porn', although

51 See the Dutch 2016 instruction for prosecuting CSAM offences.

established as an umbrella term for the intended phenomenon, no longer fully covers the broad connotation of manifestations such as online shaming, the unwanted publication of sexual imagery, or the creation or distribution of pornographic deepfakes, which we discuss below.

In the latter cases, we are then more inclined to speak of 'abuse of sexual imagery', 'online shaming', 'shame sexting' or the 'non-consensual sharing of sexual material'. Research shows that in 2023, for example, 0.4% of Dutch people had experienced this abuse of sexual material.[52] This abuse of sexual imagery can take place on a very large scale, especially in so-called 'expose groups', where pictures of (often female) victims, often accompanied by personal information and personal data, are published and/or shared (see also Section 4.7.2 about 'doxing'). To illustrate, a Dutch court considered in a case how nude photos, together with the victim's Instagram and Snapchat profile, were shared on a Telegram channel with 88,215 members.[53]

Finally, we point out there is one type of sexual imagery abuse that is bound to increase in the near future: sexual deepfakes (Flynn et al., 2022; Goudsmit Samaritter et al., 2023; van der Sloot et al., 2021). The term 'deepfake' is a contraction of 'deep' and 'fake'. 'Deep' refers to deep learning and machine learning algorithms used to create the material, while 'fake' emphasises the inherent artificiality of the material. The underlying technology used by this software to create deepfakes are called 'generative adversarial networks' (Goodfellow et al., 2020). This technology was immediately abused to create non-consensual sexual deepfakes of celebrities (McCosker, 2022).

Case study: 'deepnudes' on Reddit

In 2017, the faces of U.S. celebrities such as Taylor Swift and Gal Gadot were put on the bodies of porn actresses (called a 'face swap'). These videos first circulated on the platform Reddit. Reddit user '/u/ deepfakes' was a user of the subreddit (a kind of internet forum) '/r/ deepfakes'. This subreddit was dedicated to sharing 'non-consensual sexual deepfakes' and quickly gained popularity.[54]

52 CBS, *Security monitor 2024*, p. 52.

53 Court of Midden-Nederland 1 February 2022, ECLI:NL:RBMNE:2022:294.

54 S. Cole, 'AI-Assisted Fake Porn Is Here and We're All Fucked', *Motherboard*, 11 December 2017.

In February 2018, Reddit banned this sexual deepfake subreddit. This example was followed by other popular platforms, such as Discord (a chat platform), Pornhub (a pornographic website), X (formerly Twitter, a microblogging service) and Meta (formerly Facebook, a social media service).[55] Research shows that the number of non-consensual sexual deepfakes is rapidly increasing and mainly targeting women as the subject of sexual deepfakes (Flynn et al., 2022; Pascale, 2023).

In 2023, 'generative AI apps' became extremely popular. These apps generate 'new' content and not just manipulate material. Through a command (a 'prompt'), the software receives an instruction to generate text, images, audio, or video. The misuse of these apps became evident, for instance, when deepfakes of Taylor Swift were distributed on platform X on 25 January 2024. These images received 45 million views and 24,000 reposts within 17 hours until it was removed by the platform.[56]

Criminalisation

The Convention on Cybercrime does not specifically address the non-consensual sharing of sexual material. However, the EU Directive on combating violence against women specifically criminalises sexual deepfakes in Article 5 as 'non-consensual sharing of intimate or manipulated material'. Member States must criminalise the publication of materials depicting sexually explicit activities or the intimate parts of a person, without that person's consent, where such conduct is likely to cause serious harm to that person. Producing, manipulating or altering these materials and subsequently making it accessible to the public, without that person's consent, where such conduct is likely to cause serious harm to that person, must also be criminalised.

The abuse of sexual imagery or deep fakes may also be criminalised as the expression offence 'libel', where someone's honour or good name is attacked with the apparent aim of making it public (see also Section 4.7.2). Van der

55 A. Hern, '"Deepfake" face-swap porn videos banned by Pornhub and Twitter', *The Guardian*, 7 February 2018 and D. Hawkins, 'Reddit bans "deepfakes" pornography using the faces of celebrities such as Taylor Swift and Gal Gadot', *The Washington Post*, 8 February 2018.

56 J. Weatherbed, 'Trolls have flooded X with graphic Taylor Swift AI fakes', *The Verge*, 25 January 2024.

Hof (2016) explains that this may be the case, for example, when a revenge porn photo of an ex is posted online with accompanying texts via chat, on internet forums or on social media. The offence may include cyber-dependent aspects, such as the hacking into an online storage system (such as iCloud or OneDrive) or secretly taking images from a webcam using malware. When minors are involved, crimes such distributing CSAM may be applicable or producing or distributing virtual CSAM, when these images are morphed pictures or deepfakes of a minor.

4.6.4 Sextortion

Sextortion is a contraction of the words 'sex' and 'extortion' and refers to the use of sexually explicit images as a means of blackmail (Wolak & Finkelhor, 2011). For example, sextortion occurs when the victim is first enticed to show (e.g. via webcam) or send a nude image, after which these webcam recordings or images are used to force the victim to perform more – possibly more and more far-reaching – sexual acts in front of the webcam, and there are threats that the images will be disseminated over the internet. It also occurs that the victim is forced to pay money or provide other (sexual) services. The difference with unwanted sexting and non-consensual sharing of sexual material is that threats are used to force a victim to do something, even if the distribution of the images never takes place (Wolak et al., 2018).

Case study: the webcam extortionist

Aydin C., also known as the 'webcam extortionist', gained international notoriety after the suicide of 15-year-old Canadian Amanda Todd in 2012.[57] She was driven to such despair as a result of C.'s practices that she decided to end her life. Her YouTube video 'My story: Struggling, bullying, suicide, self harm' about this received worldwide attention. The Royal Canadian Mounted Police initiated a criminal investigation. Aydin C. became a suspect in a Dutch criminal case, after Facebook's security department forwarded a report to law enforcement authorities about a possible offender of child abuse. After some time, Dutch authorities traced back Aydin C. location because of an IP address which led to a recreational park in the Netherlands.

57 See CBC, 'The Sextortion of Amanda Todd', 15 November 2013.

Aydin C. took a sophisticated approach. He used 86 aliases on Facebook to entice 34 underage women and five adult men to take nude videos or photos of themselves after which he extorted them and forced them to provide him with new material. In doing so, he posed as an underage boy. Aydin C. also used for extorted five men with images of them masturbating. They thought they were webcamming with an underage boy. He made use of a virtual webcam program called 'Manycam' and a voice distortion program, which allowed him to pretend to be someone else.[58] In case of non-payment, the offender would distribute the images to friends and family. He hid his IP address with a virtual private network (VPN) connection (see Chapter 9) and misused passports of others to register with the online payment service 'Skrill'. Finally, he used the Western Union payment service to collect the sums (totalling more than €30,000) he had obtained through webcam extortion.[59]

In 2018, the Amsterdam Court of Appeal sentenced Aydin C. to ten years and eight months in prison for the 'sextortion' of his victims.[60] He was also prosecuted and sentenced in Canada for extorting and harassing Amanda Todd. The Canadian was sentenced thirteen years in prison and was commuted to (another) six years prison sentence by the Dutch court.[61]

Criminalisation

In the Aydin C. case, his behaviour was classified by the courts as (online) sexual assault and extortion. His victims often did not have any way to prevent the offender from distributing the images and therefore felt compelled to give in to the perpetrator. Most states will criminalise such behaviour as sexual abuse or extortion. In this case, there is also (attempted) remote sexual assault involved. Thus, sexual assault possibly does not require physical contact between the perpetrator and the victim; it can also take place from a distance (through the internet).

58 J. Proctor, 'Accused in Amanda Todd cyberbullying case alleged to have used 22 accounts to sextort teen', *cbc.ca.*, 6 June 2022.

59 Court of Amsterdam 16 March 2017, ECLI:NL:RBAMS:2017:1627, *Computerrecht* 2017/103, annotated by J.J. Oerlemans (*Aydin C.* case).

60 Amsterdam Court of Appeal 14 December 2018, ECLI:NL:GHAMS:2018:4620.

61 Court of Amsterdam 23 December 2023, ECLI:NL:RBAMS:2023:8234.

Sextortion is criminalised as 'cyber-harassment' in Article 7 of the EU Directive on violence against women (see also Section 4.7.2). The Convention on Cybercrime does not specifically criminalise sextortion. However, when a minor is involved in sextortion, CSAM is likely an offence. Note that cyber-dependent crimes may also apply when the offender uses malware to hack into the victims' computers in order to obtain more material.

4.6.5 Online grooming and sex chatting

Online grooming can be defined as the online encapsulation of a minor with the intention of sexually abusing the child or producing CSAM (Lindenberg & van Dijk, 2016; de Hingh, 2018).

In literature, grooming can be described as a (lengthy) process (crime script) in which the groomer goes through a series of time-sequential phases (O'Connell, 2003). These phases relate to friendship formation, relationship formation, risk assessment, exclusivity and the sexual phase. However, research also suggests that the course of online grooming can vary greatly and that the time groomers spend on each phase can vary greatly (e.g. some groomers enter the sexual phase almost immediately) (Gorissen et al., 2020).

Still, the general picture is that after the first encounter with a minor, the potential groomer slowly gains the child's trust through (frequent) chat or email contact, entices them to share certain intimacies and thus makes them susceptible to sexual abuse in the physical world.[62] Grooming behaviour thus consists mainly of communication, and from that language – for example, sexual innuendos in the chat, text or email conversations – it will often (have to) appear that the perpetrator's ultimate aim is to commit sexual abuse in the real world (de Hingh, 2018; 2023).

Criminalisation

In criminal law, online grooming often represents a type of criminal acts preparatory to 'offline' abuse of children (UNODC, 2013). In the Lanzarote Convention it was criminalised as 'a proposal, through information and communication technologies, of an adult to meet a child who has not reached the age of sixteen with the intention of engaging in sexual activities, where this proposal has been followed by material acts leading to such a meeting'.[63]

62 *Dutch Parliamentary Papers II* 2008/09, 31810, no. 3, pp. 6-7.
63 See Art. 23 of the Lanzarote Convention.

Grooming is not specifically criminalised in the Convention on Cybercrime. However, when during grooming, a minor is engaged in sexual activities or genitalia are exposed via a webcam, this may trigger CSAM offences. When payments are involved, offences such as child prostitution may apply. Finally, if the perpetrator exposes himself or herself, masturbates, or forces or coerces the victim to do or undergo sexual activities, this may constitute corruption of minors or even sexual assault (Schermer et al., 2016).

Case study: 'Sweetie 2.0: the virtual decoy'

Sweetie 2.0 was a chatbot with the appearance of a Filipino girl. This virtual decoy was developed and deployed by the children's rights organisation Terres des Hommes in 2013 in their fight against the phenomenon of webcam sex with minors in the Philippines. This virtual decoy allowed men guilty of this offence to be caught red-handed (van der Hof et al., 2019). About 20,000 men from some 71 countries sought contact with Sweetie 2.0. In the ten-week period of the project, approximately 1,000 suspects could be identified and handed over to their home country's investigative authorities based on personal data and Facebook details.[64]

It can be difficult to prosecute a case like Sweetie for two reasons. The first problem is that since Sweetie is not a real person, countries must have criminalised virtual CSAM or sexual abuse not with a real, but 'realistic person' in their domestic laws. In addition, offenders may be prosecuted for grooming, but then the behaviour must be criminalised in which there is a proposal to meet a – not necessarily real – person below sixteen years old.

This kind of criminal case also makes for a challenging criminal investigation, because live webcam performances leave few traces and there is little evidence that law enforcement can use. Further difficulties arise from the fact that webcam sex tourism often has a trans-border character, which causes jurisdictional conflicts and makes

64 F. Huiskamp, 'Voor het eerst man veroordeeld vanwege chatten met virtuele meisje sweetie' ['Man convicted for the first time for chatting with virtual girl sweetie'], *NRC Handelsblad*, 21 October 2014.

it more difficult to obtain evidence or even launch an investigation (see Schermer et al., 2016; see also Chapter 9).

4.7 Online expression offences

A growing body of literature focusses on different types of expression offences such as hate speech. Authors examine, among other things, the nature and extent of hate speech, but also at what makes online hate speech substantially different from offline hate speech (see, for example, Bakalis, 2018; Brown, 2018; Chetty & Alathur, 2018; Citron, 2014; Mathew et al., 2019). Online hate speech refers to discriminatory expressions shared through the internet, targeting historically marginalised people based on their inherent characteristics. Criminalised types of hate speech usually target gender, religion, race and physical disabilities (Chetty & Alathur, 2018).

The internet facilitates expression offences such as hate speech, because content can be shared quickly with little to no monitoring on social media platforms through retweets, reposting and copying hate speech. In addition, the content is available to large audiences and often published anonymously. Nave and Lane (2023) also point out that the content can easily be manipulated in ways that intensify hate (visible in, for example, hate profiles, memes and deep fakes).

The dynamics of anonymity and online disinhibition are also pivotal in understanding the proliferation of expression offences on the internet (see further Chapter 8). This phenomenon also underscores the intricate relationship between the physical and the digital world. For example, a breeding ground for a conflict may arise while chatting or interacting on internet forums, which then may result in face-to-face threats. Conversely, a conflict between people may arise in the physical world, and then result in hate speech and harassment online (van Wilsem, 2010).

While it is clear what is meant by hate speech and other expression offences, determining its criminality can be difficult. To examine this further, we first elaborate on how criminalisation and prosecution for expressions can be at odds with the right to freedom of expression in Article 10 of the European Convention on Human Rights (ECHR). Our discussion then

extends to specific offences outlined in the first protocol of the Convention on Cybercrime and EU regulations, shedding light on the nuances of their prosecution.

4.7.1 Freedom of expression vs. criminalisation

Any encroachment upon an individual's freedom of expression entails an interference with the freedom of expression laid out in Article 10 of the ECHR. Article 10 ECHR is referred to by McGonagle (2020) as 'the centrepiece of protection for the right to freedom of expression in Europe'. Access to information through the internet is recognised as an integral aspect of this fundamental right, alongside the right to publish information.[65] The European Court of Human Rights (ECtHR) underscores the internet's vital role in enhancing public access to news and facilitating the dissemination of information in general.[66] Consequently, measures such as website blockades are viewed as constraints on freedom of expression, thus interfering with the freedom of expression.[67]

An interference with the freedom of expression, is problematic because this fundamental right is seen as a prerequisite for the functioning of a democracy and for the implementation of an effective system of human rights.[68] Moreover, too broad criminalisation of expression offences can lead to abuse and (self-)censorship for fear of criminal consequences.[69] According to the ECtHR, in a democracy there should also be room for expressions that 'offend, shock or disturb'. Information and ideas must be allowed to circulate

65 ECtHR 1 December 2015, nos 48226/10 and 14027/11, ECLI:CE:ECHR:2015:1201JUD004822610, paras 52-54 (*Cengiz v. Turkey*). See also ECtHR 16 December 2012, no. 3111/10, ECLI:CE:ECHR:2012:1218JUD000311110, para. 50 (*Ahmet Yildirim v. Turkey*).

66 See, for example, ECtHR 16 June 2015, no 64569/09, ECLI:CE:ECHR:2015:0616JUD006456909, para. 133 (*Delfi v. Estonia*).

67 ECtHR 1 December 2015, nos 48226/10 and 14027/11, ECLI:CE:ECHR:2015:1201JUD004822610, paras 59-67 (*Cengiz v. Turkey*). See also T.E. McGonagle, in his annotation to: ECtHR 23 June 2020, no 20159/15; 10795/14, ECLI:CE:ECHR:2020:0623JUD002015915; ECLI:CE:ECHR:2020:0623JUD001079514 (*Kharitonov v. Russia*) & (*Bulgakov v. Russia*), *EHRC Updates* 2020, 'Court stands firm on excessive nature of IP-address blocking'.

68 See, for example, ECtHR 7 December 1976, no. 5493/72, ECLI:CE:ECHR:1976:1207JUD000549372, para. 49 (*Handyside v. UK*), ECtHR 15 October 2015, no. 27510/08, ECLI:CE:ECHR:2015:1015JUD002751008, para. 196 (*Perinçek v. Switzerland*), and ECHR 26 March 2016, no. 56925/08, para. 48, ECLI:CE:ECHR:2016:0329JUD005692508 (*Bédat v. Switzerland [GK]*).

69 This is also called the 'chilling effect'.

to safeguard the 'pluralism, tolerance, and broadmindedness without which there is no "democratic society"'.[70] At the same time, the ECtHR is also aware of the downside of unrestrained freedom of expression and signals the danger of a rapid spread of hate speech by use of the internet.[71]

When assessing whether an interference with the right to freedom of expression amounts to a violation of the right, the ECHR applies a standard test. It first establishes whether the impugned measure that has led to the interference with the right to freedom of expression is prescribed by law. Second, it determines whether the impugned measure pursues a 'legitimate aim' as mentioned in Article 10(2) ECHR.[72] Third, it assesses whether the measure is necessary in a democratic society, corresponding to a 'pressing social need'. The measure must be proportionate to the legitimate aim(s) pursued and the reasons given by state authorities for the measure must be 'relevant and sufficient'. The Court interprets the adjective 'necessary' in a strict fashion (see Janssens & Nieuwenhuis, 2019; McGonagle, 2020).

4.7.2 Criminalisation of online expressions

States often criminalise certain expressions as criminal acts, such as defamation, slander, incitement, doxing, and hate speech. These offences are briefly discussed below. However, it is crucial to acknowledge that pursuing civil procedures under civil law is often a better alternative for victims, rather than resorting to criminal prosecution through law enforcement. Criminal law is, after all, an 'ultimum remedium' with severe penalties such as imprisonment for offenders (Kesar, 2018). The ECtHR also emphasises in case law that prosecution of crimes of expression in criminal law should be limited to necessary, serious cases.[73] For many victims, seeking recourse through litigation may offer a satisfactory resolution, by demanding compensation, rectification, or removal of illegal materials.

70 ECtHR 7 December 1976, no 5493/72, ECLI:CE:ECHR:1976:1207JUD000549372, para. 49 (*Handyside v. UK*).

71 ECtHR 16 June 2015, no 64569/09, ECLI:CE:ECHR:2015:0616JUD006456909, para. 110 (*Delfi v. Estonia*).

72 These interests in Art. 10(2) ECHR are as follows: national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

73 ECHR 20 November 2006, No 47579/99, ECLI:CE:ECHR:2006:0420JUD004 757999, paras 46 and 50 (*Raichinov v. Bulgaria*).

Defamation and slander

Criminal defamation involves an expression offence where an individual's reputation is tarnished, casting them in an unfavourable light. Slander distinguishes itself from defamation by the deliberate dissemination of false claims by the offender (while knowing it to be untrue). In many countries slander carries graver penalties compared to defamation.

Determining the punishability of an expression is not always straightforward. This complexity arises partly from the need to contextualise the conduct within the prevailing societal norms and 'time-bound social attitudes', as noted by de Hullu (2018). The question of whether an expression is punishable necessitates a thorough examination of the specific circumstances, guided by the above-mentioned three-step test of the ECtHR. In certain instances, the public interest and freedom of expression may prevail over the alleged punishability of the expression. Speech sometimes warrants protection, even if the expression itself is deemed offensive, particularly when it contributes to the social debate. In cases of defamation, the offender of defamation must then be able to assume in good faith that his statement is true and that the public interest demands the accusation. Should the freedom of expression prevail over the interest of the victim of the defamation, acquittal or dismissal of all charges should follow.

Criminal defamation hinges on the requirement that the expression occurs 'in public'. However, defining what constitutes 'public' is often ambiguous in the digital realm. For example, is sharing a message or image in a closed group on a communication app or a private profile on social media 'public' or not? The size of a group app or circle of persons to whom the expression was made is often an important factor in determining whether the expression was made in public.

Incitement

Incitement is a criminalised expression wherein an individual encourages others to commit a crime or to engage in violent actions against a public authority. In numerous jurisdictions, including the Netherlands, it is not required that the offence or violence actually materialises; what matters is the *danger* that it might take place. In the Netherlands, this offense of incitement carries a much higher prison sentence (up to five years), compared to other expression offences (often with one- or two-year maximum prison sentences).

The EU Directive on combating violence against woman and domestic violence defines 'cyber incitement to violence or hatred' as 'intentionally inciting violence or hatred directed against a group of persons or a member of such a group, defined by reference to gender, by publicly disseminating, by means of ICT, material containing such incitement'.[74] EU Member States must make such incitement punishable as a criminal offence, but may choose to punish only when it is carried out in a manner likely to disturb public order or when it is threatening, abusive or insulting.

By criminalising certain expressions such as incitement, governments try to counter these statements in order to maintain public order. Certain expressions may lead to aggression or violence, and criminalisation may be required to protect the reputation of persons and to protect the human dignity and equality of persons or groups of persons. The roots of the criminalisation of the insult of groups or group discrimination, lie in the 1930s, during the growth of fascism and antisemitism in Western Europe (van Noorloos, 2012). In the Netherlands, for example, many of these offences are also expanded over time to comply with international treaties and for societal reasons. These expansions aim to safeguard the unimpeded social cohesion of groups and ensure individuals' rights to feel like integral members of society, shielding them from discriminatory expressions (de Ruiter & Velleman, 2023).

Case study: The Base

'The Base' is a neo-Nazi accelerationist paramilitary group and training network and consists of an international network of right-wing extremists. It advocates the formation of 'white ethnostates', a goal which it believes it can achieve via terrorism and the violent overthrow of existing governments. In this case study, several supporters of 'The Base' were active in Telegram groups and viewed themselves as a resistance group against a Jewish-dominated political system.[75]

74 Art. 8 of the Directive.

75 This case study is based on the judgment of Court of Rotterdam 2 December 2021, ECLI:NL:RBROT:2021:11858 and the following media reports of Cyril Rosman, 'Jonge rechts-extremisten opgepakt vanwege terreurverdenking, nazispullen ingenomen' ['Young, right extremists detained for terrorist offences'], *Het Parool*, 30 October 2020 and 'Nederlandse aanhangers "rassenoorlog" hoeven niet terug de cel in' ['Dutch supporters "race war" do not need to go back to jail'], *Het Parool*, 2 December 2021.

In Telegram groups called 'Youth Storm' and 'Beau Sneatcha', and a WhatsApp group called 'J.S.N.', extreme messages were posted by supporters of The Base. The defence argued that with regard to the Telegram group Youth Storm, the accused should be acquitted, because it was a closed group and the expressions did not take place in 'public'. The court determined that despite the small sizes of the groups Youth Storm and J.S.N. with respectively 21 and 30 participants, they collectively formed a single public entity. Consequently, expressions made within these groups were deemed to be within the public domain. Beau Sneatcha's statements were evidently part of this public discourse. In this group, they called for violence and/or the killing of people of colour, homosexuals, and Jews. In the Telegram group Youth Storm, the accused further incited to murder and abduct pedosexuals. The accused also encouraged another participant in his desire to carry out a similar attack as Brenton Tarrant did on two mosques in Christchurch, New Zealand, killing 51 people. Instead, the accused suggested a synagogue for such an attack.

The Court of Rotterdam considered that an attack on a (Jewish) house of worship is undeniably incitement with terrorist intent. In the WhatsApp group J.S.N, the accused was also found guilty of incitement, because calls were made to kidnap persons of colour, which fits into the ideology of right-wing extremist accelerationism, and can therefore also be considered a terrorist offence. In this case, the accused was sentenced to two years' imprisonment (of which 18 months were conditional), 200 hours of community service and a three-year probation.[76]

Doxing

Doxing is the publication of personal information of a victim by means of IT, without the victim's consent, for the purpose of inciting other persons to cause physical or serious psychological harm to the victim. The recent EU Directive on combating violence against women and domestic violence, includes the criminalisation of doxing as a type of 'cyber-harassment'. In the EU Directive, cyber-harassment is defined as 'repeatedly or continuously engaging in threatening conduct directed at a person, at least where such

76 Court of Rotterdam 2 December 2021, ECLI:NL:RBROT:2021:11858.

conduct involves threats to commit criminal offences, by means of ICT, where such conduct is likely to cause that person to seriously fear for their own safety or the safety of dependants'.[77] The recent EU Directive (adopted in 2024), criminalises widespread manifestations of 'cyberviolence', including the non-consensual sharing of intimate images (including deepfakes), cyber-stalking, cyber-harassment, misogynous hate speech and 'cyber-flashing' (e.g. 'dick pics'). According to the EU, the criminalisation will help victims of these types of cyberviolence in Member States that did not yet criminalise these acts.

The above highlights how various types of expression-related offences often intersect, as well as the interwovenness of the physical world and the digital world. Furthermore, the justification for criminalisation and prosecution of such offences must adhere to the three-step test outlined by the ECtHR. For instance, the Dutch legislator considers that, in context of journalistic publications, there is no intent to commit doxing, and therefore no criminal conduct and no prosecution should be brought.[78] Additionally, in instances of doxing, emphasis is placed on prioritising alternative (preventative) measures over prosecution. These measures include 'first and foremost': promoting a safe online environment, raising awareness, and removing the data through the (internet) host of the medium or civil proceedings (see Section 4.7.3). It is imperative for the Public Prosecution Service to consider these factors in formulating its prosecution policies (Nan & Schemer, 2023).

Hate speech

McGonagle (2020) states that a 'red line' of protected expression can be clearly identified around the contours of 'hate speech'. This typically falls under Article 17 ECHR (referring to the abuse of rights, including expression). There is no (legal) definition of hate speech available, but in the past, the court has applied Article 17 to ensure that Article 10 protection is not extended to racist, xenophobic, or antisemitic speech, and (neo-)Nazi ideas, and statements denying, disputing, minimizing, or condoning the Holocaust (McGonagle, 2020). Hate speech can cause different harms, including physical, psychological and socio-economic harm (Delgado, 2019).

77 Art. 7. See also Recital 24 about doxing.

78 *Parliamentary Papers II* 2021/22, 36171, no. 3, p. 9.

The First Protocol of the Convention on Cybercrime (adopted in 2003) obliges states to criminalise certain types of hate speech.[79] The drafters of the protocol were concerned by the risk of misuse or abuse of computer systems to disseminate racist and xenophobic propaganda. In 2024, only 35 states ratified the Additional Protocol to the Convention on Cybercrime, a notably lower figure compared to the 72 ratifications of the Convention itself. The aim of the Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems is twofold. Firstly, it seeks to harmonise substantive criminal law in the fight against racism and xenophobia on the internet. Secondly, it aims to enhance international cooperation in addressing these issues.[80] When countries criminalise certain behaviours similarly, judicial cooperation and legal assistance is often more straightforward.

'Racist and xenophobic material' is defined in the First Protocol as 'any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors'.[81] Note that this definition does not encompass gender and sexual orientation. The EU Directive on combating violence against women and domestic violence specifically includes the criminalisation 'cyber-incitement' to violence or hatred based on gender.[82]

Put briefly, the First Protocol urges member states to criminalise or (when committed intentionally and without right): (1) *distributing*, or otherwise making available, racist and xenophobic material to the public through a computer system; (2) *threatening* persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or a group of persons which is distinguished by any of these characteristics; (3) publicly *insulting* the aforementioned persons or groups of persons; and finally (4)

79 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28 January 2003, ETS no. 189. See also Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law 2008, OJ L 328.

80 Explanatory report of the First Protocol, para. 3.

81 See Art. 1 of the First Protocol.

82 See Art. 8 of the Directive on combating violence against women and domestic violence.

distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting *genocide* or *crimes against humanity*.[83]

4.7.3 Removing illegal content

In numerous countries, governmental authorities have the power to remove illicit content. Given the interference with the freedom of expression, in the Netherlands for example only a judge can give this order, upon request of a public prosecutor for specific (serious) crimes (Oerlemans, 2017b).[84] The idea is that the order will only be issued, if the provider has not complied with a request for a notice and takedown (on a voluntarily basis). The police or a public prosecutor can request the removal of illegal content or request to make the content inaccessible, just like everyone else. They can use the 'takedown power' when the request is not complied with.

With regard to the takedown order, the Digital Services Act (DSA) (adopted by the EU in 2022) is particularly relevant.[85] This Regulation imposes diligence requirements for providers of intermediary services to tackle illegal content. The most important provisions entail an obligation to take down illegal content upon receiving an order by the relevant national judicial or administrative authorities, on the basis of the applicable Union law or national law in compliance with Union law.[86] Furthermore, the DSA imposes an obligation on hosting services to put in place 'notice and action mechanisms'.[87] These mechanisms allow users – both users in general and users with a particular interest, such as 'trusted flaggers' – to report the presence of (allegedly) illegal content to the service provider concerned. Trusted flaggers are entities that have shown to have the necessary expertise and objectivity to submit reliable notices and are therefore officially designated, at their request, as trusted flaggers by the competent national authorities. The INHOPE network of hotlines for reporting child sexual abuse material is an example of a trusted flagger.[88] Providers of online platforms

83 See Art. 3-6 of the First Protocol.

84 See Art. 126p Dutch Code of Criminal Procedure Law and Art. 67 of the Dutch Code of Criminal Law.

85 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), PbEU 2022, L 277/1.

86 Art. 9 DSA.

87 Art. 16 DSA.

88 Recital 65 DSA.

are required to handle notifications submitted by so-called 'trusted flaggers' with priority.[89] Providers are expected to take prompt action and remove the information following a request, insofar specific conditions are met (Wilman, 2022).[90]

Whether illegal content is removed following a notification, depends on several factors. Technical limitations may hinder the removal of data, and strained relationships with service providers or differing jurisdictional regulations can further complicate matters (van Hoboken et al., 2020). For instance, the Dutch government has highlighted the strained relationship between Telegram and the Dutch police, posing challenges in blocking Telegram channels and identifying its users (see further Chapter 9).[91] Additionally, law enforcement agencies have raised concerns about 'bulletproof hosting providers', who, due to their revenue model, are reluctant to remove material from their servers promptly, often delaying or only removing content after notifying customers (Europol, 2023).

The guiding principle for the issuance of takedown orders is proportionality, ensuring that the exercise of power is warranted by the severity of the harm caused and balanced against the right to freedom of expression. In the Netherlands, this is reflected in a step-by-step approach, gradually encroaching on freedom of expression only when the interests of the victims outweigh the preservation of free speech. First, law enforcement authorities should urge the individual who posted the unlawful material to remove the material. If this proves unsuccessful or the poster is uncooperative, authorities may approach website owners. Should this step also prove ineffective, authorities may turn to hosting providers. As a last resort, internet access providers may be compelled to render content inaccessible by implementing an 'internet filter'. In the Netherlands, this measure is rare. The only example is that Vodafone/Ziggo and KPN are mandated to block access to 'The Pirate Bay', following civil proceedings based on copyright infringements.[92] It is important to recognise that the implementation of

89 Recital 61 and Art. 22 DSA.

90 These rules codify earlier case law of the CJEU, such as CJEU 12 July 2011, C-324/09, ECLI:EU:C:2011:474 (*L'Oréal v. eBay*) and CJEU 22 June 2021, C-682/18 and C-683/18, ECLI:EU:C:2021:503 (*YouTube*).

91 Parliamentary letter of a former Dutch Minister of Justice and Security, 'Telegram does not take effective action against large-scale sharing of contact details and nude photos of women', 11 October 2023.

92 Dutch Supreme Court 29 June 2018, ECLI:NL:HR:2018:1046 and Court of Appeal Amsterdam 2 June 2020, ECLI:NL:GHAMS:2020:1421.

internet filters or content blocking represents a serious interference with the freedom of expression. It is conceivable these measures will also be considered to counter not only online hate speech as discussed in this paragraph, but also other phenomena such as online gambling and online sexual offences, as discussed in section 4.6.

4.8 Future developments

In this last section, we discuss two future developments that are likely to play a role in cyber-enabled crime in the future, namely the increasing use of AI and 'virtual reality'.

4.8.1 AI and cyber-enabled crime

The increasing use of AI has already been discussed several times in this book. Chapters 2 and 3, for instance, already revealed that AI can increasingly play a role in developing malware and making it undetectable. It was also discussed that cybercriminals most likely will use 'Large Language Models' (LLMs), such as ChatGPT, to write highly convincing phishing emails or hold conversations with victims in order to carry out scams. Europol (2023) also highlights the potential of AI to create deepfakes and other synthetic media (such as audio fakes). As noted earlier in this chapter, famous (often female) individuals have already fallen victim to sexual deepfakes or audio fakes. Scholars also warn of other dangers of deepfakes, such as their use in generating disinformation during elections (van der Sloot et al., 2021). Expression offences, such as defamation, discrimination and incitement, can also be committed on a larger scale and automated with the help of AI.

Finally, Europol (2023) also points to the rise of 'dark LLMs', which are hosted on the dark web and provide a chatbot without any security, as well as LLMs that are trained on certain – particularly harmful – data, such as sexual materials from minors. Investigators will need to prepare for this, including by raising awareness and developing skills to use this technology themselves for their own job performance.

4.8.2 Crime in virtual reality and mixed reality worlds

A very different development that will most likely play out in the cyber domain in the future is the role of 'augmented' and 'virtual reality' (also

called 'immersive reality' and 'extended reality'). In augmented reality, our perception of the world is extended by adding virtual elements to reality, for example through devices such as smartphones, augmented reality glasses or games such as 'Pokémon Go'. In virtual reality, the physical world is (in whole or partly) replaced as much as possible by an artificial or virtual reality, for example through virtual reality glasses.

Legal research suggests that the current legal framework in countries such as the Netherlands is well-equipped to address the potential negative effects of immersive technology (Schermer & van Ham, 2021). However, it is important to point out that that victims of virtual sexual assault experience similar emotional reactions to a physical sexual assault or rape. Schermer & van Ham expect that as the immersion and sense of presence in a virtual environment increases, the impact of virtual transgressive behaviour may also increase. These technologies raise new questions, for example whether virtual assault or virtual vandalism should be better criminalised (Strikwerda, 2014; ten Voorde, 2017).

4.9 To conclude

This chapter has explained the main types of cyber-enabled crime, namely: offences facilitated by online marketplaces, money laundering with virtual currency, online fraud, online sexual offences and online expression offences. You will now understand the ways in which these crimes are usually committed and how they are generally criminalised. As we have seen, in practice, both cyber-enabled and cyber-dependent crimes apply simultaneously. Cybercriminals are often highly specialised and work together to make money. For example, it is possible to commit fraud after financial personal data is copied through computer hacking using malware. The money earned by fraud can then be laundered using virtual currencies. Different criminals have different roles to make this possible. Therefore, it also illustrates the reality of 'hybrid' (cyber) criminal networks (see further Chapter 6).

We have also seen that the criminalisation of many behaviours, especially when it comes to expression crimes, is not always easy to answer. The question of whether an expression is punishable must be answered based on a concrete situation and balanced with the right to freedom of expression. Criminal law is also not always the best tool to combat harmful expressions.

4.10 Discussion questions

1. Is the distinction between cyber-dependent crime and cyber-enabled crime always clear?
2. In what types of crime do you observe a clear interconnection of the offline and online world?
3. Is it appropriate to criminalise the phenomenon of 'sex chatting'?
4. Is cyber-harassment criminalised in your country?
5. Do you agree with the government that crypto money is not 'real' money?
6. Are sexual deepfakes sufficiently criminalised?
7. Does the criminalisation of sexual offences sufficiently do justice to the possible suffering experienced in the virtual world?
8. Should rape in a virtual world be punishable similarly as rape in the physical world?
9. Does this book rightly classify expression offences as cyber-enabled crime?
10. Is criminal law the best tool to combat expression offences?
11. What type of cyber-enabled crimes deserves more research and for what reason?
12. After reading this chapter, what do you think of the statement: 'The law always lags behind technological developments'?

4.11 Key concepts

- Bitcoin
- Child sexual abuse materials (CSAM)
- Cyber-enabled crime
- Cyber harassment
- Cyber stalking
- Dark web
- Darknet market
- Ddos attack
- Deep web
- Deepfake
- Defamation
- Discrimination
- Doxing
- Expression offences
- Incitement

- Grooming
- Identity fraud
- Money laundering
- Non-consensual sharing of sexual material
- Online criminal marketplaces
- Online fraud
- Online hate speech
- Revenge porn
- Sexting
- Sextortion
- Take down request
- Tor
- Virtual currencies