Tackling Cyberscams through EU Criminal Law

*Professor Alisdair A. Gillespie[[1]](#footnote-1)\**

*Lancaster University*.

# I. Introduction

Fraud is one of the oldest forms of crime. It remains remarkably resilient to attempts at eradicating it. The internet has given it a new lease of life, with new opportunities to scam people. Cyberfraud has quickly become the dominant form of fraud, with global losses accounting for billions of euros a year.[[2]](#footnote-2) Indeed, the number of reported cases is so large that some law enforcement agencies struggle to investigate all reports.[[3]](#footnote-3)

While many Western countries have seen a decline in traditional property crimes, cyberfraud has significantly increased.[[4]](#footnote-4) Potentially this is because the risk of detection is lower than conventional property crime, but also due to the nature of the crime. It provides opportunities to scam people worldwide, with physical borders swept away by digital technologies.

Despite this, it will be seen that EU criminal law rarely specifically addresses the issue of cyberfraud against its citizens.[[5]](#footnote-5) This chapter will initially present some key forms of cyberfraud before assessing how EU criminal law addresses these behaviours. Finally, the chapter considers how the transnational reach of cyberfraud challenges enforcement. The chapter concludes that this is an area where the EU should do more, including through greater harmonisation of laws.

# II. Cyberfraud

This chapter focuses on scams rather than large-scale corporate fraud. In essence, the focus will be on fraud against individuals. While recognising this is a controversial limitation, a key aim of EU criminal law is to protect EU citizens.[[6]](#footnote-6) The consequences of cyberfraud are so significant as to justify the use of the criminal law.

Classifying cyberfraud can be problematic because new opportunities to scam people are created as technology develops. However, one of the more popular classifications is by Stabek et al., who identified seven categories.

1. *Fraud through low-level trickery* (simple scams that could include, for example, advertising non-existent products).
2. *Fraud through developed story-based application* (where the scam involves participating in a fraudulent narrative).
3. *Participation through employment*-*based strategies* (a person being scammed into believing that completing a task (e.g. an online test, paying a vetting fee etc.) will lead to an employment opportunity).
4. *Fraud through implied necessary obligation* (e.g. purchasing software without being informed subscriptions will auto-renew).
5. *Information gathering through authentic appeals* (where a legitimate cause (e.g. a charity or child in need) is hijacked or falsified to attract revenue).
6. *Financial gain through merchant and customer*-*based exploitation* (e.g. auction frauds, the selling of counterfeit goods or where a buyer pretends not to have received the goods).
7. *Financial gain through marketing opportunities* (effectively get-rich scams such as 'Ponzi' schemes).[[7]](#footnote-7)

While extensive, this list is perhaps limiting. It presents, in essence, modern examples of existing behaviour. The scams listed above have existed for many years. While much cyberfraud is simply an electronic version of pre-existing behaviour, this is not always true. For example, 'formjacking' is where malicious code is embedded within legitimate sites allowing credit card details to be captured or diverting a legitimate money transfer. Ransomware locks a user out of their device unless a ransom is provided. Some would argue that these are not frauds *per se* but are instead a form of financial crime committed during a computer attack.[[8]](#footnote-8) The debate is not necessarily academic, as understanding the behaviours and their origins is essential when designing strategies to prevent fraud. Advice on avoiding ransomware will differ from that given for auction frauds.

A particular feature of cyberfraud is the ability of criminals to respond to new opportunities quickly. COVID is an example of this, as fraud increased significantly. Partly this was because so many people were working from home remotely, but also because scammers could prey on concerns.[[9]](#footnote-9) Levi notes that a significant number of cyberfrauds concerned the sale of masks and other personal protection equipment for individuals,[[10]](#footnote-10) many of which did not arrive, were sub-standard or not as described.

Quantifying cyberfraud can be challenging, partly because it is known to be underreported.[[11]](#footnote-11) This could be because victims believe the sums lost are negligible, they lack understanding of how to report the matter, or they are too embarrassed to do so.[[12]](#footnote-12) Reep-van den Ergh and Junger analysed nine national crime surveys across the EU. They found a victimisation rate of between 2.2% and 3.5%.[[13]](#footnote-13) This is lower than other researchers who suggest that victimisation is more like 7%.[[14]](#footnote-14) To put that into context, 7% of the population of the EU would be upwards of 32 million people.

## A. Consumer Fraud

The first type of cyberfraud to consider is consumer fraud. This is one of the more common forms of cyberfraud[[15]](#footnote-15) even though many trading platforms (e.g. eBay, Craiglist, Etsy and Amazon) devote considerable resources to tackling fraud on their platforms.[[16]](#footnote-16)

Three common forms of consumer fraud include:

* auction frauds,
* counterfeit goods,
* missing goods.

Missing goods is self-explanatory, so no more will be said about that. Counterfeit goods have existed for a long time, but the global e-market has led to a resurgence. Indeed, the EU Commission has argued that counterfeiting is now a significant activity for organised crime whereas, they claim, it was previously the preserve of relatively small organisations.[[17]](#footnote-17)

The nature of e-commerce poses particular challenges for tackling counterfeiting. Unlike in a physical shop, the consumer cannot inspect the goods before purchase to check they are legitimate. That said, it can be questioned whether all those who purchase counterfeit goods are victims of fraud. There has always been a market for 'fake merchandise' where people are prepared to pay for a replica of goods they cannot afford. Perhaps the classic examples of this have been designer luggage and watches,[[18]](#footnote-18) but it can include other luxury goods such as antiques and writing instruments.

Criminal organisations have expanded counterfeiting beyond consumer goods, and, notably, there is now a strong market for counterfeit health products, including medicines.[[19]](#footnote-19) This demonstrates a particular challenge with counterfeiting. The wrong in counterfeiting is not just IP violations but can include physical risks. Counterfeits tend to be poorly made and rarely adhere to product standards. This can pose significant risks to the health of consumers.

Auction frauds are prolific. While the principal online auction sites devote considerable resources to preventing fraud, the nature of the business model means that some fraudulent activity is inevitable. Of course, where an auction site has a global reach, even a minuscule percentage can equate to millions of euros lost through fraud.[[20]](#footnote-20)

A simple form of auction fraud is not sending the goods. While it may be thought that this is only an issue for large-value items, it need not be. Low-value items can be as profitable to a fraudster. Let us assume that X purchases a book from an auction site, winning the bid at €2,50. The item does not arrive after 10 days. What does X do? Some will contact the seller, but many may write off the €2,50 thinking it is not worth the hassle. If the seller does not respond, will they escalate a €2,50 dispute to the auction site or online payment provider? Some will but many will not.

€2,50 does not seem like a lot of money, but if the seller sells' 50 items spread across various auctions, it becomes a €125 fraud. If this happens daily, the scam is worth c.€3,750 and c.€45,000 after a year. Even if a small number asks for a refund, many will not, so the 'seller' clears a significant profit.

Other types of auction frauds are more technical. For example, 'shill bidding' involves a seller creating a fake profile to try and provoke a bidding war.[[21]](#footnote-21) Bid shielding is the opposite, where a person places an unrealistically large bid to put people off bidding. The offer is then withdrawn, typically meaning the only remaining legitimate bid is a small opening bid placed by the scammer.

## B. Advance Fee Frauds

One of the oldest and most well-known scams is the advanced fee fraud, also known as a ‘419 fraud'.[[22]](#footnote-22) Most people will have sight of an advanced-fee fraud even if they have not fallen for one. The classic example is the 'Nigerian Prince' email, where a person is contacted by someone who needs to move money out of the country due to corruption. They are told that if they allow their account to be used, they can retain the interest or receive a percentage of the transfer.[[23]](#footnote-23)

A contemporary example of an advanced-fee fraud relates to prizes. A person is told that they have been pre-selected to win a prize in an online competition (typically based on their email address, telephone number or postcode). Sometimes a convincing website is created to show that it is legitimate, although often it is just a basic email. The 'winner' is told that they need to either formally enter the contest or pay an administration fee to release their (valuable) prize.[[24]](#footnote-24)

It seems extraordinary that advance-fee scams can ever succeed. The emails that set out the scam are often poorly worded,[[25]](#footnote-25) so they should be easily spotted. The emails are spam and are sent to vast numbers of people. The fraudsters work on the basis that all they require is a few people to respond. They rely on greed. That people's greed will make them see past the story's absurdity. Their confidence is well-placed, with advance-fee scams costing millions of euros yearly.[[26]](#footnote-26)

## C: Confidence Scams

When one thinks of a 'scam', it is difficult not to conjure up the idea of the hustler—the smart-suited conman who tries to charm their victim into participating in some scheme. Hustles exist on the internet and are one of the more successful forms of cyberfrauds. While there are several different confidence scams, two of the most common are romance and investment fraud.

Investment frauds have become particularly significant in recent years, perhaps reflecting that interest rates have been historically low in most Western countries. In Australia, for example, it was noted that investment scams accounted for the biggest losses, estimated at nearly AU$330m in 2020 alone.[[27]](#footnote-27) Similarly, in the UK, it has been stated that investment frauds are the number one cyberfraud threat.[[28]](#footnote-28) It was estimated that c.14% of respondents to the EU Commission survey on fraud had experienced investment fraud.[[29]](#footnote-29) Europol has stated that investment fraud became the dominant type of confidence fraud in 2021.[[30]](#footnote-30)

While there are different types of investment frauds, they typically offer a non-existent product that promises gains beyond that which could be achieved through traditional investments. The fraudster will not infrequently go to extreme lengths to persuade investors to part with their money. The fraud can involve face-to-face meetings, the production of professional-looking websites, spreadsheets and testimonials. It may take several months for the fraud to come to fruition, but the scammer is likely to have several scams on the go simultaneously.

Romance frauds also remain popular. Carter has argued that they are analogous to child grooming.[[31]](#footnote-31) Indeed, there is some similarity. The fraudster ultimately seeks to persuade the victim that they are in a romantic relationship and that the monies the fraudster seeks are for their mutual benefit or future.[[32]](#footnote-32) While some scams will take place solely online, others will involve physical meetings and even physical intimacy. The victim may believe they are in a committed relationship and can even introduce the scammer to their family.

A significant problem with confidence fraud is victim-blaming. It is not uncommon for people to describe a victim as 'stupid' and for friends and, in particular, family to resent the victim for falling for the scam.[[33]](#footnote-33) This acts as additional victimisation and frequently leaves the victim without support or having to deal with hostility from those close to them.

## D: Phishing

Phishing is another well-known cyberfraud. Put simply, it is where a person is tricked into disclosing, for example, their bank or credit card details. A common form of phishing is an email requiring a person to 'confirm' their bank details, often because a suspected fraud has occurred. While historically, these emails, as with 419 frauds, were extremely basic and often easily spotted, they have become more sophisticated. Scammers are producing emails that look legitimate, often containing links such as 'how do I know this is not a scam'. Other links embedded within the emails will take people to the legitimate website, establishing trust.

A particularly nasty type of phishing is when the scammer pretends to work for a bank or the police. They contact the victim to explain that they suspect their account is the subject of fraud. They wish to catch the fraudster – who is suspected of working in the bank – and so they need to transfer all monies into a 'clean' account. Due to the fraudster being an insider, they are told not to talk to anyone about the operation. As the victim believes they are talking to the police, the sums lost can be substantial.

Analogous to phishing is diversion fraud. These have become popular, and it is where a scammer persuades someone to divert a legitimate payment into a different bank account. This is particularly prevalent in house sales, where the sums can be significant. On or around the completion date, an email is received from the lender or lawyer that the payment for the property has to be sent to a different bank account. Often the email says that this is because the company has been the subject of a cyberattack or fraud, meaning that they need to use a 'clean' account. Due to the inevitable stress involved in moving and completing a house sale, victims do not necessarily check whether the email is legitimate. This can lead to hundreds of thousands of euros lost in a single transaction.

## E: Ransomware

The essence of ransomware is that a trojan is installed on the target computer, often after clicking on a contaminated link or email. The trojan will typically encrypt the device and display a message informing the user that they cannot access the device unless they pay a ransom, usually paid via cryptocurrency, to make identification difficult.

In most instances, the encryption is so powerful that it is impossible to remove it, rendering the device useless. Whether to pay the ransom is controversial. It can be argued that it is futile to do so because there is no guarantee that the device will be unlocked. The counter-argument is that the business model of ransomware requires the device to be released. If devices are never recovered, then why would anyone pay the ransom? Research suggests that both schools of thought are valid, with at least some devices not being unlocked despite the ransom being paid.[[34]](#footnote-34) Of course, the difficulty for the victim is that it is impossible to know in advance who will release the device and who will not.

Europol has noted that the number of ransomware attacks across Europe continues to increase, with the attacks becoming more sophisticated.[[35]](#footnote-35) However, they also said that the attacks are shifting away from private individuals to high-value targets, including public-sector bodies and large companies. That is not to say that ransomware attacks are no longer dangerous to private individuals. Still, it reflects the reality that significant money can be made by attacking corporations or government bodies.

# III. EU Legislative Response

EU criminal law is a relatively new phenomenon, with the EC/EU not having formal competence in this area until the Maastricht Treaty.[[36]](#footnote-36) The Lisbon Treaty created a new constitutional structure for the EU, including staking an interest in criminal justice matters. Article 83(1) of the *Treaty on the Functioning of the European Union* (TFEU) provides that the EU has competence to 'establish minimum rules concerning the definition of criminal offences and sanctions' albeit in respect of limited areas. The primary limitation is that it must be a 'serious crime with a cross-border dimension'. An (exhaustive) list is then produced, which is 'terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime'.

One of the key points to note is the reference to 'minimum rules'. It is sometimes said that the purpose of EU legislation is to harmonise the criminal law of member states, but it has been noted that this is an elusive concept and that 'approximation' is a better term.[[37]](#footnote-37) This means that the Member States are left to define the offences under national law, but the EU establishes a set of minimum principles that all national laws must abide by. Member States can go beyond these minimum principles but cannot do less. A framework is then established that provides a minimum set of safeguards throughout the Union.

While the Member States will set the maximum sentence for the crime, the EU legislation will establish a term below which the maximum penalty cannot fall. For example, the Directive on combating fraud[[38]](#footnote-38) proposes an offence of the fraudulent use of a stolen non-cash instrument.[[39]](#footnote-39) The Directive states that the maximum sentence for this offence should be no less than two years imprisonment.[[40]](#footnote-40) Member States could set their (domestic) maximum punishment at two years or, for example, five years, and both would be compliant. A Member State could not, however, set the maximum term at 18 months' imprisonment. That said, doubt remains over how easy it is for the Commission to enforce compliance with criminal law legislation.[[41]](#footnote-41)

It will be remembered that the EU only claims competence under Article 83 for specific offences.[[42]](#footnote-42) Fraud is not one. While the EU has sought to use criminal law to target fraud, it has tended to be directed towards fraud against the EU itself, its budget and its currency.[[43]](#footnote-43) What of cyberfraud? 'Computer crime' is mentioned in Article 83(1). Is 'computer crime' the same as cybercrime? This is an oft-debated question,[[44]](#footnote-44) partly because we have preconceived ideas about a 'computer'. As will be seen, for our purposes, the distinction is arguably superfluous because the wording of the legislation is sufficiently wide to encompass other technologies.

There is not a single EU legislative instrument that seeks to tackle cyberfraud. Instead, reliance must be placed on multiple instruments. While the Commission has suggested using some civil law instruments,[[45]](#footnote-45) these will not be considered in this chapter because our focus is on criminal law, which has the greater potential to deter inappropriate behaviour.

## A: Counterfeiting

Counterfeited goods pose a significant risk to the single market; thus, early on, the EU introduced legislation to tackle it. The earliest instrument was a Regulation that sought to limit their circulation.[[46]](#footnote-46) However, despite this and subsequent legislation, the amount of counterfeited goods reaching the EU has continued to increase.[[47]](#footnote-47)

The current Regulation[[48]](#footnote-48) primarily focuses on the holders of intellectual property rights and not on individuals. Therefore, person X who unwittingly purchases counterfeit goods cannot rely on the Regulation to seek the prosecution of the seller. The holder of the intellectual property can use the Regulation to seek the enforcement of its property rights by national customs enforcement, but only large corporations will likely use this.

The EU Commission proposed harmonising criminal law for counterfeiting, but the proposal received a lukewarm reception from Member States, and it never came to fruition.[[49]](#footnote-49) A new effort began after the signing of the *Lisbon Treaty*, with the Kingdom of Belgium convening a conference to consider harmonisation.[[50]](#footnote-50) Again, there was sympathy and recognition that every Member State did not necessarily understand the difficulties of counterfeited goods. Once again, no legislative action was forthcoming, meaning that it remains an issue ultimately for the Member States.

## B: Computer Attacks

It was noted above that ransomware could be considered more analogous to an attack. That being the case, EU law arguably treats it more seriously. As far back as 2001, the EU recognised that hacking and other computer attacks posed a risk to the Union.[[51]](#footnote-51) This was followed in 2005 by a Framework Decision that sought to harmonise the laws of Member States.[[52]](#footnote-52) In common with other Framework Decisions, it had mixed success,[[53]](#footnote-53) and after the passing of the Lisbon Treaty, it was replaced with a Directive.

The Directive on attacks against information systems[[54]](#footnote-54) seeks to synchronise laws across Europe by prohibiting, *inter alia*, the illegal access to information systems,[[55]](#footnote-55) illegal system interference[[56]](#footnote-56) and illegal data interference.[[57]](#footnote-57)

At the heart of the Directive is the concept of an 'information system', which is defined as:

a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically process computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance.[[58]](#footnote-58)

Whilst a complicated definition, it suffices to note that computers, tablets and other such devices would fall within it.

Article 3 prohibits 'the access without right, to the whole or any part of an information system'. The principal aim of this offence is to tackle hacking, but for our purposes, Articles 4 and 5, which relate to system interference, are more relevant.[[59]](#footnote-59) Article 4 prohibits an information system's 'hindering or interrupting' by transmitting, deleting or suppressing data. Article 5 is very similar, but the attack's object is the data itself. While it has been said that the distinction between them is obscure,[[60]](#footnote-60) ransomware may help illustrate the difference. Where a computer is encrypted and ransomed, Article 4 would apply because the information system has been interfered with. Where, however, the relevant data was stored in the cloud and access to this data – rather than the device –has been blocked, then Article 5 could apply.

One issue of controversy is that the Directive allows Member States the right not to criminalise minor attacks.[[61]](#footnote-61) The Directive does not define what 'minor' means, and Summers notes that the Commission is sceptical about what constitutes a minor attack.[[62]](#footnote-62) Certainly, given the repercussions of a ransomware attack, it is hoped that this would never be considered minor, and each report is investigated as a crime.

## C: Other Frauds

While counterfeiting and ransomware are covered by specific legislation, the position in respect of other cyberfrauds are more complicated. The principal legal instrument of relevance is the Directive on combating fraud and counterfeiting of non-cash means of payments.[[63]](#footnote-63)

The recital to the Directive notes that cyberfraud can threaten the Union's security and act as an obstacle to the digital single market.[[64]](#footnote-64) Both of these justify why the EU believes that cyberfraud should be tackled. Importantly, and in contrast to the systems attack Directive, the recital notes that even small-value frauds should be tackled as part of a coherent strategy to combat cyberfraud effectively.[[65]](#footnote-65) This must be welcomed since, as indicated in Part II of this chapter, small-scale frauds can sometimes mask larger-scale frauds.

The Directive requires Member States to create five substantive offences together with an offence of inciting, aiding, abetting and attempting a substantive offence.[[66]](#footnote-66) Those offences are:

* Fraudulent use of non-cash payment instruments (Article 3).
* Offences related to the fraudulent use of corporeal non-cash payment instruments (Article 4).
* Offences related to the fraudulent use of non-corporeal non-cash payment instruments (Article 5).
* Fraud related to information systems (Article 6).
* Tools used for committing offences (Article 7).

The Directive is aimed at 'non-cash payment instruments', defined as:

a non-corporeal or corporeal protected device, object or record, or a combination thereof, other than legal tender, and which alone or in conjunction with a procedure or set of procedures enables the holder or user to transfer money or monetary value, including through digital means of exchange.[[67]](#footnote-67)

This is a somewhat technical definition, and a better definition is given by the European Central Bank, which provides examples of cards, credit transfers, direct debits and e-money. This also helps us contextualise 'corporeal' and 'non-corporeal' instruments. An example of a corporeal instrument would be a debit or credit card. It is a physical instrument that can be used to transfer money from one account to another. A non-corporeal instrument would include direct debits, standing orders, money transfers and cryptocurrencies.

It may be thought that restricting the Directive to non-cash payments is necessary to ensure it falls within the definition of 'computer crime' in Article 83(1) TFEU. However, that is not necessarily the case since a traveller's cheque must be a (corporeal) non-cash payment, yet a fraud relating to these may not involve a computer. Conversely, cash payments are outside the scope and cause difficulties even when a computer is used.

**Example A**

D persuades V that they are a police officer and that they are investigating internal misconduct at a bank. D requires V's assistance and asks him to withdraw €5,000 and hand it to them.

**Example B**

D persuades V that they are a police officer and that they are investigating internal misconduct at a bank. D requires V's assistance and asks him to transfer €5,000 out of his savings account into a 'clean' account.

In both examples, V loses €5,000. However, only example B is within the scope of the Directive. Yet the actual fraud is the same in both examples. It seems unjust because, in example A, the victim hands over cash, no EU offence is committed. It may be thought that such examples would be always be covered by domestic law, but it demonstrates perfectly the disjointed approach adopted to cyberfraud.

### Article 3

Article 3 criminalises the fraudulent use of a stolen, counterfeit or falsified non-cash payment instrument. It is perhaps less relevant to our discussion, although it would include someone using a cloned credit card to make purchases on the internet.

### Articles 4 and 5

Article 4 prohibits the unlawful appropriation of a corporeal non-cash payment, its counterfeiting or falsification. It also prohibits the possession of a stolen or counterfeited instrument. Thus, while Article 3 prohibits their use, Article 4 essentially prohibits their acquisition or possession. Article 5 is very similar but relates to non-corporeal non-cash payments. It prohibits their unlawful obtainments, counterfeiting or falsification. Article 5 allows the unlawful obtainment to be restricted to those situations where they were obtained in a way that breaches the attack on information systems Directive discussed earlier. In other words, when they are obtained by hacking or interfering with an information system. However, it is submitted that it would be better for Member States to take a broad approach to Article 5 to tackle scams and not just those instances that arose from an attack.

Whether Article 4 or 5 applies will depend on how the financial transaction is made. Where it is a bank transfer or an online payment transfer (e.g. PayPal, Apple Pay etc.) Article 5 will be relevant. If a person uses a debit or credit card to pay online, then Article 4 will apply. Since Articles 4 and 5 effectively mirror each other, any loopholes should be minimised.

Article 4(b), which criminalises the counterfeiting or falsifying of a corporeal non-cash instrument, could also be useful when a person uses payment details to clone a credit or debit card. Most online purchases require a user to include the 16-digit card number, expiry date and the security code. With these details and others easily obtained, criminals can clone the card. These can then be sold to others or used to make purchases.

Article 5(b), which relates to the falsification of non-corporeal instruments, potentially assists in respect of diversion frauds. It will be remembered that one form is that the purchaser of a home etc., is told at the last minute to send funds to a different account, ostensibly due to potential fraud.[[68]](#footnote-68) This should fall within Article 5(b) as the new details have been falsified. The scammer is pretending to be the legitimate recipient of the money and subsequently falsifies the payment request so that the money is diverted.

Sadly, Articles 4 and 5 are unlikely to assist with advance-fee frauds and confidence scams. In neither of these types of fraud can it be said that there is misappropriation or falsification of either a corporeal or non-corporeal non-cash payment *instrument*. There is no doubt that the financial loss suffered by the victim is obtained inappropriately, but the victim in both types of scams consciously chooses to transfer the money. It cannot be said that the instrument was stolen, counterfeited or falsified. The accompanying story was undoubtedly false, but the actual transaction is entered into willingly (albeit caused by a deception). By focusing on the instrument rather than the financial loss, the Directive fails vulnerable members of society who have been tricked.

### Article 6

Article 6 prohibits the transfer of money (or equivalent) by hindering or interfering with an information system or computer data. This overlaps considerably with Article 5, where, it will be remembered, the Directive makes a cross-referral to the information systems attack Directive. Perhaps the most significant difference between Articles 5 and 6 is that Article 6 requires an actual loss whereas Article 5 does not; it criminalises the obtaining of the instrument, but no loss may be caused by its procurement; the loss may not occur until the instrument is executed.

Article 6 could be helpful in the context of ransomware. While, as was seen earlier, the Directive on attacks on information systems will apply to the hacking and encryption of the device, it does not directly deal with the ransom. Where a ransom is paid, Article 6 would apply as the ransom equates to an actual financial loss. This acknowledges that a ransomware attack involves two wrongs – the technical attack and the ransom – and the criminal law should address both.

Article 6 may also assist where technical attacks alter the infrastructure of websites. So-called DNS pollution attacks are where a hacker uses malware to redirect people away from a legitimate website to a site designed, for example, to capture the payment details.[[69]](#footnote-69) The victim believes that they have made a legitimate purchase or transfer, not realising that the payment has, in fact, been diverted to the fraudster. This must be considered hindering or interfering with computer data, meaning Article 6 would apply.

# IV: Jurisdiction and Mutual Legal Assistance

The legislative instruments discussed above should provide a framework to tackle some forms of cybercrime. However, by itself, it will not be sufficient. Like most cybercrime, the biggest obstacle to tackling cyberfraud is jurisdiction. The internet knows no (physical) borders. It is as easy for someone in France to defraud a person in Sweden as it is to someone in France. Indeed, it is arguably preferable to do so because law enforcement may be reticent to investigate an incident in another country.

## A: Jurisdiction

The traditional rule of jurisdiction is territoriality.[[70]](#footnote-70) That is to say, a state is free to prescribe rules that apply within its territory and will not usually prescribe rules that apply outside of its borders. For example, it would be unusual for Croatia to develop a law that says that smoking on the streets of Paris is illegal. Under the territoriality principle, Croatia could ban smoking on the streets of Zagreb, but it should not prescribe conduct in Paris, leaving that to the French government.

Territoriality helps to ensure that there is no conflict of laws. If we return to the smoking example, if both France and Croatia prohibited smoking on the streets of Paris, then if someone did smoke a cigarette, would they be tried in France or Croatia? The general principle is that a person should not be tried twice for the same facts,[[71]](#footnote-71) so the choice of jurisdiction can be important.

A key question posed of territorial jurisdiction is where the crime takes place. The classic dilemma is where D and V stand on either side of a (land) border. D shoots V dead. Does the murder occur where D pulls the trigger or V dies? This dilemma also exists in cyberspace. D, a resident of Germany, lists an item for sale on the internet but never intends to deliver it. V, a resident of the Netherlands, purchases it. Does the fraud occur in Germany (where the item was listed) or the Netherlands (where the loss of money occurred)?

Even if the location is properly identified, territoriality poses other problems. If a country does not extradite its own citizens, then if the offender has left the country where the crime occurred, the chances of them standing trial there is low. Further, some countries may not have as developed a legal system, which can cause challenges. The classic example often given is in respect of so-called Child Sex Tourism.[[72]](#footnote-72) As the laws in some Asian countries were ineffective or not enforced appropriately, citizens of wealthy countries would travel to Asia and abuse children once there. The risk of detection or prosecution was lowand therefore seen as a 'safe' activity. They did not need to worry about the laws of their own country because the crime took place outside of its borders.

In some instances, a state may choose to act in an extraterritorial manner, i.e. it will decide that its national laws will extend to acts that take place outside of its borders. Historically there have been two approaches. The first is to use the 'active personality principle'.[[73]](#footnote-73) This is where the actions of its citizens (or, on occasion, those habitually resident in their territory[[74]](#footnote-74)) can be tried in their national courts even though the conduct took place outside of its territory. The second principle is the 'passive personality principle'.[[75]](#footnote-75) This is where a state claims the right to try persons who commit acts against their citizens (or those habitually resident) even though the acts did not take place within its territorial borders.

Given the internet's borderless nature, it has become increasingly common for national and international legal instruments to address jurisdiction expressly. Article 12 of the Directive on non-cash payments requires Member States to establish jurisdiction where the offence is committed in whole or in part of its territory, or where the offender is one of its nationals. This addresses both territorial and extraterritorial jurisdiction.

The reference to 'whole or in part' is designed to resolve the conflict about where a crime occurs. This can be particularly relevant in respect of remote attacks:

D, a citizen and resident of Italy, has created malware that allows him to undertake ransomware attack. To protect his identity, he uses malware to infect computers in Latvia and Romania. He uses one of the Latvian computers to launch a ransomware attack on three computers in Poland.

In the example above, D may seek to claim that Italy (where he lives) has no jurisdiction to try him because the attack took place in either Latvia or Poland. However, Article 12(2) clarifies that Italy can claim jurisdiction as part of his actions took place there. Indeed, in the example above, Italy, Latvia and Poland would all be able to claim jurisdiction.[[76]](#footnote-76)

Of course, 'in whole or in part of its territory' can go beyond where the computer, suspect or victim is. It could also include where any money is transferred to. So, for example, D (a citizen of France) defrauds V (a citizen of Estonia) out of €600 and transfers the sum to an account he has created in Sweden. In this example, France, Estonia and Sweden could all claim jurisdiction.

A common failure of instruments that seek to extend jurisdiction is that they rarely say who has first claim on the suspect. This is true of the fraud Directive. Although it addresses jurisdiction, it does not say who should take the lead. Other parts of the Directive require Member States to cooperate and exchange information, but it does not clarify who has first claim.

It may be thought that the State that has custody of the suspect should go first, but it is not necessarily that simple. While the state may have custody of the suspect, does it have the evidence? If the victim is based abroad, as is much of the technology, then it may be difficult for the state to prosecute. It is no easier if the country where the victim is present goes first. While they will have easy access to the victim (and their computer), they do not have custody of the offender or their computer.

## B: Mutual Legal Assistance

In 2018 over one-half of investigations involved a cross-border request for electronic information.[[77]](#footnote-77) If anything, it is likely that this figure will have increased due to the popularity of ICT. How then does a prosecuting state gather evidence from outside of the jurisdiction? This takes us into the territory of mutual legal assistance (MLA).

An immediate distinction must be drawn between MLA that takes place wholly within the EU and MLA involving a non-member state. Within the EU, obtaining custody of a suspect is easier because of the European Arrest Warrant[[78]](#footnote-78) and obtaining evidence of investigation support is facilitated by the European Investigation Order.[[79]](#footnote-79) The latter empowers a judicial authority to issue an order requiring a Member State to gather and transfer evidence to the requesting law enforcement agency. While simpler, there continue to be concerns that the process remains cumbersome and unsuited to fast-moving cybercrime investigations.[[80]](#footnote-80) Indeed, there have been proposals for a new EU instrument on electronic evidence[[81]](#footnote-81) that will seek to improve the position.

The transient nature of digital evidence causes difficulties for law enforcement agencies who can find that service providers have deleted the data they require before they make contact. The EU introduced a requirement for providers to retain communications data[[82]](#footnote-82) but in *Digital Rights Ltd. v Minister for Communications, Marine and Natural Resources and others[[83]](#footnote-83)* the Court of Justice of the EU declared the Directive incompatible with EU law. This has significantly impacted some countries, with the absence of communications data impeding several investigations.[[84]](#footnote-84) That said, it is equally clear that several Member States have ignored the ruling,[[85]](#footnote-85) creating a patchwork that is unhelpful to law enforcement across the EU. Attempts are ongoing to reconcile these difficulties, but it remains a complex and controversial area.

Aside from legislation, the EU has sought to encourage MLA. In 2017, Project SIRIUS was established.[[86]](#footnote-86) This project, coordinated by both EUROPOL and EUROJUST, provides resources that assist law enforcement in accessing data through MLA. It also assists agencies in obtaining data that may be accessible within their territory (e.g. where a device is connected to the cloud). One of the aims of SIRIUS is to ensure that all Member States have the same technical abilities, and that countries with perhaps less domestic expertise can access specialist assistance.

Where MLA becomes complicated is where the organisation possessing the evidence is outside of the EU. While the EU has some bilateral agreements,[[87]](#footnote-87) they do not replicate the regime within the EU. The agreements try to simplify matters but they will invariably constitute a compromise between the competing demands of different jurisdictions. Often, the bilateral agreements are old and not fit for the demands of modern digital investigations,[[88]](#footnote-88) which can raise challenges for investigators.

One challenge for MLA outside of the EU is a lack of commonality over requests and information sought. Each jurisdiction has their own forms, guidance and rules. It has been noted that INTERPOL has attempted to develop a system that will help standardise MLA requests, including providing a secure system to exchange requests and data. However, this has not yet been fully implemented.[[89]](#footnote-89)

MLA is not always between state agencies. For example, the USA permits companies to answer requests for MLAs, at least for non-content data.[[90]](#footnote-90) Accordingly, an LEA could contact an online service provider (e.g. Facebook) directly, rather than have to seek the assistance of, for example, the Department of Justice or the American courts, which could slow the matter down. However, such cooperation is arguably voluntary, at least when no subsidiary is based within a member state. The provider will also need to adhere to national laws, making investigations based on content challenging in the USA where the First Amendment treats hate-crime matters differently to, for example, European instruments.[[91]](#footnote-91)

There is some evidence that law enforcement agencies find MLA challenging outside of the EU, including with the USA. The Third Annual Report of the SIRIUS project considered responses from law enforcement agencies across the EU.[[92]](#footnote-92) Nearly half of respondents stated that they found the MLA process took too long, and over 40% noted that a key challenge was that companies all had different policies and processes.[[93]](#footnote-93) The report specifically considered MLA requests to the USA (where many online service providers are based). 40% of respondents noted that requests were denied due to conflicts with the First Amendment to the US Constitution.[[94]](#footnote-94) The reason why this can be problematic is because of the principle of dual-criminality. The intra-EU system requires that Member States recognise the laws of another Member State. However, outside of the EU it is common for treaties to require dual criminality before they will take action. This is the rule that requires an act to be illegal in both the requesting and providing states. For certain matters, most notably content issues such as hate-crime or pornography, this can be problematic because the First Amendment will protect material that is illegal in many European countries, effectively stymieing the chances of successful MLA.

# V: Conclusion

As the EU has itself recognised, cyberfraud has the potential to undermine the internal market of the EU. This is true of small-scale frauds where, for example, retail fraud makes consumers wary about making purchases online. E-commerce will continue to grow and thus consumers must have confidence that they will not be scammed during purchases.

It is submitted that the EU does not treat cyberfraud seriously enough. It is an area where greater harmonisation of laws would be of benefit. The non-cash payments directive is a start, but there are too many areas that fall outside of it. Also, its language is clumsy and causes confusion. A new directive should be passed that seeks to target the most common forms of cyberfraud. If implemented, this would provide a framework of protection across the EU.

Digital evidence has become routine but accessing it can remain problematic. The current arrangements for MLA do not work and their revision is necessary. The proposed legislation on electronic evidence is crucial and should be expedited. There must be common approaches to the gathering, analysis and disclosure of electronic evidence, at least within the EU. Coupled with more appropriate MLA protocols, this could provide an effective way of ensuring that those who use the internet to defraud people will be held to account.

1. \* Some of the research used in this chapter was previously gathered by Samantha Magor, then Research Assistant at Lancaster University Law School, for an earlier piece on fraud. The author wishes to acknowledge the invaluable assistance of Samantha. [↑](#footnote-ref-1)
2. Majid Yar and Kevin F. Steinmetz, *Cybercrime and society* (3rd edn, SAGE 2019) at 129-130. [↑](#footnote-ref-2)
3. Alisdair A. Gillespie, *Cybercrime: Key Issues and Debates* (2 edn, Routledge 2019) at 314). [↑](#footnote-ref-3)
4. Steven Kemp, Fernando Miró-Llinares and Asier Moneva, ‘The dark figure and the cyber fraud rise in Europe: evidence from Spain’ (2020) 26 European Journal on Criminal Policy and Research 293 at 294. [↑](#footnote-ref-4)
5. Historically it has focused on fraud against its budget etc. [↑](#footnote-ref-5)
6. Sarah J Summers and others, *The emergence of EU criminal law: Cyber crime and the regulation of the information society* (Bloomsbury Publishing 2014) at 47 et seq. [↑](#footnote-ref-6)
7. Amber Stabek, Paul Watters and Robert Layton, *The seven scam types: mapping the terrain of cybercrime* (IEEE 2010) at 44-45. [↑](#footnote-ref-7)
8. Discussed in Alisdair A Gillespie and Samantha Magor, ‘Tackling online fraud’ (2020) 20 ERA Forum 439. [↑](#footnote-ref-8)
9. See, for example, Katelyn Wan Fei Ma and Tammy McKinnon, ‘COVID-19 and cyber fraud: emerging threats during the pandemic’ (2021) 29 Journal of Financial Crime 433 who argue cogently that the psychological context of COVID must be taken into account when understanding the reasons why fraud occurred during this time (at 434-5). [↑](#footnote-ref-9)
10. Michael Levi, ‘Fraud, Pandemics and Policing Responses’ (2021) SCE 5 European Law Enforcement Research Bulletin 1 at 3. [↑](#footnote-ref-10)
11. Yar and Steinmetz, n 1 above, at 144. [↑](#footnote-ref-11)
12. Gillespie, n 2 above, at 104. [↑](#footnote-ref-12)
13. Carin MM Reep-van den Bergh and Marianne Junger, ‘Victims of cybercrime in Europe: a review of victim surveys’ (2018) 7 Crime Science 1. [↑](#footnote-ref-13)
14. Kemp et al, n 3 above; Monica T Whitty, ‘Predicting susceptibility to cyber-fraud victimhood’ (2019) 26 Journal of Financial Crime 277. [↑](#footnote-ref-14)
15. Yar and Steinmetz, n 1 above, at 131. [↑](#footnote-ref-15)
16. Gillespie, n 2 above, at 157. [↑](#footnote-ref-16)
17. Benjamin Farrand, ‘“Alone we can do so little; together we can do so much”: the essential role of EU agencies in combatting the sale of counterfeit goods’ (2019) 28 European Security 22 at 27. [↑](#footnote-ref-17)
18. See, for example, Gail Tom and others, ‘Consumer demand for counterfeit goods’ (1998) 15 Psychology & Marketing 405. [↑](#footnote-ref-18)
19. Jonathan Harper, *Counterfeit medicines: Survey Report* (2006, Council of Europe). [↑](#footnote-ref-19)
20. Yar and Steinmetz, n 1 above, at 131. [↑](#footnote-ref-20)
21. Gillespie, n 2 above, at 157. [↑](#footnote-ref-21)
22. ‘419 frauds’ are so-named because this is the section of the Nigerian Criminal Code that was written to tackle such scams. Historically, Nigeria was responsible for a considerable amount of these scams. [↑](#footnote-ref-22)
23. Thomas J. Holt and Danielle C. Graves, ‘A qualitative analysis of advance fee fraud e-mail schemes’ 1 International Journal of Cyber Criminology 137 [↑](#footnote-ref-23)
24. Michaela Beals, Marguerite DeLiema and Martha Deevy, *Framework for a taxonomy of fraud* (Financial Fraud Research Center, 2015) at 11. [↑](#footnote-ref-24)
25. Holt and Grave, n 22 above, at 149. [↑](#footnote-ref-25)
26. Yar and Steinmetz, n 1 above, at 135. [↑](#footnote-ref-26)
27. *Targeting scams: report of the ACCC on scam activity* (Australian Competition & Consumer Commission, 2021) at 12. [↑](#footnote-ref-27)
28. https://data.actionfraud.police.uk/cms/wp-content/uploads/2021/07/2020-21-Annual-Assessment-Fraud-Crime-Trends.pdf (Last accessed 12.06.21). [↑](#footnote-ref-28)
29. *Survey on ‘Scams and Fraud Experienced by Consumers’ Final Report* (20202, European Commission) at p.12. [↑](#footnote-ref-29)
30. Europol, *Internet Organised Crime Threat Assessment 2021* (Publications Office of the EU, 2021) at 32. [↑](#footnote-ref-30)
31. Elisabeth Carter, ‘Distort, extort, deceive and exploit: exploring the inner workings of a romance fraud’ (2021) 61 The British Journal of Criminology 283. [↑](#footnote-ref-31)
32. For further details on how the frauds operate see Monica T. Whitty and Tom Buchanan, ‘The online romance scam: A serious cybercrime’ (2012) 15 CyberPsychology, Behavior, and Social Networking 181 and Cassandra Cross and Thomas J Holt, ‘The Use of Military Profiles in Romance Fraud Schemes’ (2021) 16 Victims & Offenders 385. [↑](#footnote-ref-32)
33. See, for example, Cassandra Cross, ‘No laughing matter: Blaming the victim of online fraud’ (2015) 21 International Review of Victimology 187. [↑](#footnote-ref-33)
34. Cath Everett, ‘Ransomware: to pay or not to pay?’ [2016] Computer Fraud & Security 8. [↑](#footnote-ref-34)
35. *Internet Organised Threat Assessment*, n 29 above, at 20. [↑](#footnote-ref-35)
36. Summers et al, n 5 above, at 5. [↑](#footnote-ref-36)
37. *Ibid*., at 259. [↑](#footnote-ref-37)
38. Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA (2019) OJ L 123/18. [↑](#footnote-ref-38)
39. *Ibid*., Article 3. [↑](#footnote-ref-39)
40. *Ibid*., Article 9(1). [↑](#footnote-ref-40)
41. See, for example, Summers, n 5 above, at 325. [↑](#footnote-ref-41)
42. Although Article 83(1) also permits additional areas to be added by unanimous vote. Politically, unanimous voting is always tricky. [↑](#footnote-ref-42)
43. Summers et al, n 5 above, at 241. Article 325 of the TFEU creates an obligation [↑](#footnote-ref-43)
44. Discussed in Gillespie, 2 above, at 1-9. [↑](#footnote-ref-44)
45. *Survey on scams and fraud*, n 28 above, at 9. [↑](#footnote-ref-45)
46. Council Regulation (EEC) No 3842/86 of 1 December 1986 laying down measures to prohibit the release for free circulation of counterfeit goods [1986] OJ L 357/1. [↑](#footnote-ref-46)
47. Farrand, n 16 above, at 28. [↑](#footnote-ref-47)
48. Regulation (EU) No 608/2013 of the European Parliament and of the Council of 12 June 2013 concerning customs enforcement of intellectual property rights and repealing Council Regulation (EC) No 1383/2003 (2013) OJ L 181/15. [↑](#footnote-ref-48)
49. Olivier Vrins, *Regulation (EU) No 608/2013 Concerning Customs Enforcement of Intellectual Property Rights* (Kluwer Law International 2018) para 73. [↑](#footnote-ref-49)
50. *Ibid*., para 75. [↑](#footnote-ref-50)
51. Summers et al, n 5 above, at 233. [↑](#footnote-ref-51)
52. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (2005) OJ L69/67. [↑](#footnote-ref-52)
53. Summers et al, n 5 above, at 239. [↑](#footnote-ref-53)
54. Directive (EU) 2013/40 of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (2013) OJ L218/8. [↑](#footnote-ref-54)
55. Article 3. [↑](#footnote-ref-55)
56. Article 4. [↑](#footnote-ref-56)
57. Article 5. [↑](#footnote-ref-57)
58. Article 2(a). [↑](#footnote-ref-58)
59. Summers, n 5 above, at 235. [↑](#footnote-ref-59)
60. *Ibid.*, at 235. [↑](#footnote-ref-60)
61. See the concluding words of each of Articles 3-5. [↑](#footnote-ref-61)
62. Summers, n 5 above, at 238. [↑](#footnote-ref-62)
63. Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting non-cash means pf payment and replacing Council Framework Decision 2001/413/JHA. [2019] OJ 123/18. As is evident from its title, this Directive replaced an earlier framework decision. [↑](#footnote-ref-63)
64. *Ibid*., Recital (2). [↑](#footnote-ref-64)
65. *Ibid*., Recital (30). [↑](#footnote-ref-65)
66. Directive 2019/713, Article 8. [↑](#footnote-ref-66)
67. *Ibid*., Article 2(a). [↑](#footnote-ref-67)
68. See p.9 above. [↑](#footnote-ref-68)
69. Gillespie, n 2 above, at 163-164. [↑](#footnote-ref-69)
70. Julia Hörnle, *Internet Jurisdiction Law and Practice* (Oxford University Press 2021) 5 and 83 et seq. [↑](#footnote-ref-70)
71. Known as *ne bis in idem* (see, for example, *ibid*., at 107 et seq). [↑](#footnote-ref-71)
72. Julia O'Connell Davidson, ‘‘Child sex tourism’: An anomalous form of movement?’ (2004) 12 Journal of Contemporary European Studies 31. [↑](#footnote-ref-72)
73. Hörnle, n 70 above, at 87. [↑](#footnote-ref-73)
74. People who reside in a territory must follow the laws of that country. Some countries decide that a person who is not a citizen but who is habitually resident in that country should be subject to extraterritorial laws. [↑](#footnote-ref-74)
75. Hörnle, n 70 above, at 88. [↑](#footnote-ref-75)
76. Technically *ne bis in idem* does not apply to different victims because each attack is a separate crime. If the charge was creating the malware then only one state could try the offender, but if the charge relates to the individual attacks or ransoms, then there is no double jeopardy. [↑](#footnote-ref-76)
77. David Wright, Krzysztof Garstka and Richa Kumar, ‘Rising to the Proliferation of Cybercrime Challenging Law Enforcement Agencies across Europe’ (2021) 21 European Police Science & Research Bulletin 81 at 86. [↑](#footnote-ref-77)
78. Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States. [↑](#footnote-ref-78)
79. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. [2014] OJ L 130/1. [↑](#footnote-ref-79)
80. Wright et al, n 80 above, at 87. [↑](#footnote-ref-80)
81. Halefom H Abraha, ‘Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives’ (2021) 29 International Journal of Law and Information Technology 118 at 129. [↑](#footnote-ref-81)
82. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks [2006] OJ L 105/54. [↑](#footnote-ref-82)
83. C-293/12; [2014] 3 CMLR 44. [↑](#footnote-ref-83)
84. For a discussion on the decision see, for example, David Fennelly, ‘Data retention: the life, death and afterlife of a directive’ (2019) 19 ERA Forum 673. [↑](#footnote-ref-84)
85. Wright et al, n 80 above, at 88. [↑](#footnote-ref-85)
86. https://www.europol.europa.eu/media-press/newsroom/news/europol-launches-sirius-platform-to-facilitate-online-investigations (last accessed 17.5.22). [↑](#footnote-ref-86)
87. See, for example, Decision 2003/516/EC on the signature of the Agreements between the EU and the US on extradition and mutual legal assistance in criminal matters [2003] OJ L181/34. [↑](#footnote-ref-87)
88. Abraha, n 84 above, at 122. [↑](#footnote-ref-88)
89. *Ibid*., at 126. [↑](#footnote-ref-89)
90. *Ibid*., at 127. [↑](#footnote-ref-90)
91. See, for example, Alisdair A Gillespie, ‘Hate and harm: the law on hate speech’ in Andrej Savin and Jan Trzaskowski (eds), *Research Handbook on EU Internet Law* (Edward Elgar Publishing 2014) (pp.488-507). [↑](#footnote-ref-91)
92. Europol, *SIRIUS EU Digital Evidence Situation Report. 3rd Annual Report.* (2021) [↑](#footnote-ref-92)
93. *Ibid*., at 22. [↑](#footnote-ref-93)
94. *Ibid*., at 39. [↑](#footnote-ref-94)