HOUSE OF LORDS

Fraud Act 2006 and Digital Fraud Committee

Uncorrected oral evidence: Fraud Act 2006 and digital fraud

Monday 6 June 2022

2.30 pm

Watch the meeting

Members present: Baroness Morgan of Cotes (The Chair); Baroness Bowles of Berkhamsted; Lord Browne of Ladyton; Viscount Colville of Culross; Lord Gilbert of Panteg; Baroness Henig; Lord Sandhurst; Baroness Taylor of Bolton; Lord Vaux of Harrowden; Lord Young of Cookham.

Evidence Session No. 16 Heard in Public Questions 171 - 178

Witnesses

I: Markko Künnapu, Legal Adviser, Estonian Ministry of Justice; Andrea Garcia Rodríguez, Lead Digital Policy Analyst, European Policy Centre.

USE OF THE TRANSCRIPT

1. This is an uncorrected transcript of evidence taken in public and webcast on www.parliamentlive.tv.
2. Any public use of, or reference to, the contents should make clear that neither Members nor witnesses have had the opportunity to correct the record. If in doubt as to the propriety of using the transcript, please contact the Clerk of the Committee.
3. Members and witnesses are asked to send corrections to the Clerk of the Committee within 14 days of receipt.

Examination of witnesses

Markko Künnapu and Andrea Garcia Rodríguez.

The Chair: Good afternoon and welcome to this latest session of the House of Lords Select Committee on the Fraud Act 2006 and Digital Fraud. A transcript of this meeting will be taken and published on the committee website, and you will have the opportunity to make corrections to that transcript when necessary. We have three sessions this afternoon. In our first session, I am delighted that we will be looking at evidence from Estonia and from the EU in relation to our inquiry. We are joined by Markko Künnapu, who is the legal adviser at the Estonian Ministry of Justice, and Andrea Garcia Rodríguez, who is the lead digital policy analyst at the European Policy Centre. Thank you both very much for joining. Without further ado, I will ask Lord Vaux to ask the first question.

Q171 **Lord Vaux of Harrowden:** Good afternoon. I would like to start with a general question. Could you us your views on the key trends that you observe in Europe and Estonia today in fraud, how this has changed over recent years, and how the counter-fraud response has evolved to keep up with the changing tactics of the fraudsters? Perhaps Andrea would start from the EU side of things and then Markko can give us a bit more detail on Estonia, if that is okay.

Andrea Garcia Rodríguez: The European Union has recently published a new set of rules dealing with online services. Those are two pieces of legislation—the Digital Markets Act and the Digital Services Act. Both of them aim at platforms that have more than 45 million active users in Europe. The difference between them is in their approaches: the Digital Markets Act targets companies that, because of their weight in the market, could impede access to other companies; the Digital Services Act, which is the one I think this committee would be more interested in hearing about, targets platforms that, because of the amount of information they handle, should have the responsibility for dealing with online fraud.

Importantly, this is a horizontal piece of legislation, meaning that it can and will be complemented by other sectoral pieces of legislation, such as the audio-visual media services directive, the directive on copyright in the Digital Services Act, the consumer protection acquis and many others that may come forward in the next months.

Europe has seen more and more users using online platforms as intermediaries for their everyday lives, be it for speaking to their relatives, buying things online or online education, especially since the pandemic. We should do something to prevent illegal activity happening in these platforms, which is something the UK is specifically worried about at the moment. That is the reason we are having this conversation now.

I have my notes here and there are plenty of things that I would like to mention about the specific file. Specifically, it is interesting for the UK that it creates not only special measures to counter illegal content online, which would be what this committee is more worried about when it comes to online fraud, but new transparency and traceability rules for sellers online. What did not appear in the draft when it was proposed in December 2020, but did appear in the final file, are special obligations for platforms to protect children online.

As a big picture, these are the things that we should discuss today. I will give the floor to Markko, who will be able to say more things about what Estonia is doing in this regard.

Lord Vaux of Harrowden: Just in terms of Europe, though, in the UK we are seeing that fraud is now the single biggest crime against individuals. Something like 42% of all crime in the UK is now fraud, and it is still growing quite quickly. Is that a dynamic that you are seeing in Europe as well, or are we an outlier in that sense?

Andrea Garcia Rodríguez: That is a general trend, not only in Europe or the UK, but everywhere in the digital world. There are 5 billion internet users every day. They use online platforms. The platformisation of everything is happening. The problem is that, the more information you put inside these platforms, the less capable you are to trace what is happening. Fraud and cybercrime are emerging trends that have been with us for a long time, but they will become more prevalent over the next few years, precisely because more people are using internet services and going online.

Lord Vaux of Harrowden: Markko, do you want to give us an overview of how things look in Estonia in terms of fraud trends and the counter-fraud response to the changing tactics?

Markko Künnapu: In Estonia, in Europe and worldwide, the key trends are similar. Looking at the figures of registered cybercrime offences, most are related to computer-based fraud or digital fraud, meaning that most cybercrime is still profit-driven, where criminals are targeting money. This has been the trend for years. In recent years, we have seen these scams and fraud schemes getting more and more complicated. Criminals have more time. They plan their attacks very carefully using social engineering. The number of victims and losses are also on the rise.

Fraud trends include investment-related fraud, lottery scams and romance scams. We have seen business emails compromised and fraud against chief executive officers. During the Covid-19 pandemic, we witnessed fraud schemes related to vaccines and medicines. At certain points, people had less physical contact, in particular during lockdown periods, and were unaware of what was happening. There were also those with carers. All of these were exploited by criminal groups.

What have the countermeasures been? Of course, a country needs to have proper legislation in place, with substantive criminal and procedural law. You need to have dedicated, responsible cybercrime units with the necessary capacity, but you also need to pay attention to overall awareness and education. It is very important to reach out to different categories of people, not only young people and children but the elderly, because these fraud schemes may target and address different population groups. Therefore, countries need to be ready. They need to provide clear messages on what to expect and what the key trends, threats and risks are.

When there is an attempt, it is important that people understand or realise that this is too good to be true, that it is suspicious and fraudulent. It is about awareness raising, education and what we like to call proper cyber hygiene—how to behave online, what to do and what one should not do.

Lord Vaux of Harrowden: We will be digging a bit further into some of those topics in a minute.

Q172 **Baroness Henig:** Good afternoon. Can I direct my question in the first instance to Markko? It is in two parts. First, how widespread is the adoption of online banking in Estonia and across the EU? Secondly, have you made any assessment of the risk from authorised push payment fraud?

Markko Künnapu: In Estonia, most banking transactions are made using electronic channels—about 98% to 99%. This has been the case for years and banks have been promoting it. In many cases, physical offices or places to do transactions have been closed. They have been pushing more and more people to use these online tools and electronic channels.

This brings certain risks. At one point, we thought that we were a bit lucky because we had more cyber-literate people, who knew how to behave online and what the risks were. Strong digital identification and authentication tools such as ID cards helped prevent these types of frauds and scams, but now we see that this might not be sufficient and that these kinds of scams can be successful. Often, people become too negligent and disclose their personal PIN codes, which are used to identify them and authenticate transactions. People may have forgotten that these codes have the same value as a physical signature. They give out this information too freely, which is why these authorised payments take place.

Then we come to investment frauds, where people who want to buy something or to invest have been deceived. They believe that the services they are using are real, but often, in these fraud cases, they are not. The problem is that once people realise that this was not a real investment company or a real investment case, time has passed and it is often difficult, if not almost impossible, to recover the money. Criminals use quite complicated schemes to move money from one account or one jurisdiction to another. Following these and conducting financial investigations can be quite difficult and, unfortunately, often not successful.

Baroness Henig: Does Andrea have anything to say perhaps about the rest of Europe? I take it, from the figures you have given, that Estonia is one of the most highly digitalised banking systems in Europe.

Andrea Garcia Rodríguez: We are seeing two trends converging here. First, as I have mentioned, more and more people are connected to the internet and using intermediary services. I am particularly concerned about the role of intermediary services. Something that we have not mentioned until now, but which will follow in the conversation, is the recent hype for cryptocurrencies. Those platforms act as intermediary services as well and we are seeing people who do not trust banks use these online services and intermediaries to make their online payments.

Secondly, something that Markko did not specifically mention, but which is contextual to our conversation, is the increase in people buying things online—e-commerce. We should be especially worried about that because, as he mentioned, like fraud, it is increasing.

How do these cybercriminals do this? Europol has seen that the most widely used technique is when people enter their credit card number and their data, and then a message appears saying, "Your card has not been found. Do it again". That is the means whereby fraud is mostly committed online, because we do not have enough mechanisms in place.

How do we avoid that? I would try to be preventive when it comes to social engineering defence, identifying social factors and points of vulnerability that cybercriminals can use to engage in these operations, entering into pre-emptive action, but also employing the right technology to do so.

I cannot say that what Markko said before is not correct. In fact, I would like to highlight what he mentioned about the value of education. People do not have enough cyber hygiene measures in place; they do not know how important it is. That is something that Estonia has done right, if I am not mistaken. Everyone should be aware that there are plenty of points of entry and that they are the first barriers to avoiding this happening. I wanted to mention all these points, because they perfectly complement what Markko said.

Baroness Henig: Do you have any idea of the percentage of online banking in, say, Germany or France?

Andrea Garcia Rodríguez: No, not specifically, but I would say that it goes beyond 70%.

The Chair: You are very welcome to write to us. We will research that, but thank you so much for that.

Q173 **Baroness Bowles of Berkhamsted:** We have already started on my question, which is to Markko, because it is mainly about Estonia. Given the higher levels of digitalisation, how are fraud and cyber defence controls built into those systems? It would be nice to hear more about that, although, from the answers just given, it seems that the cyber hygiene is breaking down a little.

To what extent does Estonia's high levels of digital literacy reduce fraud vulnerability within the general population? Again, we have already strayed into that, but, in conjunction with that, what is the level of public confidence? Are people afraid of being victims of fraud?

In an earlier response, Markko, you also said that some things had got worse during lockdown. That may be because there was more online use and online purchasing, but did I detect in what you said that a lack of social contact between people possibly increased their vulnerability in some way, or was it merely that they were buying more online? That was a bit of a rambling elaboration, but, since you have started on the core thing, I do not know whether you could add more colour there for us.

Markko Künnapu: You are absolutely right. Every year, more and more people spend time online for work or leisure, but also for e-commerce-related activities. When these limitations were in place, with a lack of physical contact, it facilitated the commission of certain types of fraud. You had no physical contact with your colleagues or superiors, and criminals were abusing this. They were sending fraudulent emails to accountants, for example, who were not able to check whether this email or this invoice was right or wrong, and who often fell into the trap. They just executed these transactions and sent money somewhere abroad, and later they identified that they had become victims of fraud and that these invoices relating to an account number were not correct.

As regards the situation in Estonia, cybersecurity and information security are a joint responsibility. The Government and the state can adopt laws and regulations establishing certain obligations, but we need to rely a lot on the private sector. When we talk about banks, once we have additional electronic services, these create lot of additional opportunities and make customers' and users' lives easier, but also bring certain risks and obligations.

Those who own or develop these services must also pay attention to the information security part. They need to protect themselves and their business models, and to pay attention to data protection. For example, at the European Union level, we have the GDPR, and there are some quite explicit obligations. Not only government authorities but private sector entities that process data need to take certain organisational and technological measures to avoid leaks and breaches. In case this happens, they could be held liable for it.

Of course, you need to just keep the systems up to date, because there are always new challenges and threats, which means that this information security and cybersecurity part needs to keep pace. The higher the digital literacy, the more people can identify these kinds of fraud, but it is still not easy to reach all the different levels or layers of the population. Unfortunately, there are still sometimes more vulnerable categories of people, and we need to think about how to reach them and improve the situation.

Baroness Bowles of Berkhamsted: In other words, in Estonia, despite a higher and earlier use of digitalisation, you are finding that there are still the same vulnerabilities as we are experiencing in the UK and elsewhere.

Markko Künnapu: Yes, that is correct. Although we have developed organisational, technical and IT-related measures to make the systems more secure, unfortunately we still have the human factor. Often, the customer or user is the weakest link and can be contacted, addressed or exploited by the criminals.

Baroness Bowles of Berkhamsted: Do the banks issue lots of warnings when you are making a transaction? Do they ask you, "Are you absolutely sure this isn't a scam?" Questions such as that now pop up when we try to transfer money electronically in the UK. Does that happen in Estonia and across the EU in general?

Markko Künnapu: Banks have their own systems and controls in place. In case of something unusual, such as where a customer has never sent money abroad and then suddenly a huge amount of money is leaving, the bank's systems could prevent the transaction. But if the person is giving full authorisation through online banking, agreeing to everything and entering all the necessary credentials and user codes, there will not be any additional warnings. If this transaction or behaviour does not match the customer profile, the internal control systems and anti-money laundering systems of the bank could intervene and prevent this, but it is the sole responsibility of the user.

Baroness Bowles of Berkhamsted: The controls that are there are more for money laundering rather than for unusual behaviour outside of money laundering. I guess a big amount of money would always perhaps prompt checks on money laundering.

Markko Künnapu: Yes, that is true, but, again, there are certain possibilities. If someone has never travelled abroad and suddenly there is some reservation on their credit card, and it seems that that transaction has been made in another part of the world, the bank's control systems would intervene. In this case, they would also contact and notify the customer and ask whether they authorised this transaction. In case they identify that there is a fraud and a criminal offence taking place, they can take necessary measures to prevent this.

Q174 **Lord Young of Cookham:** Fighting fraud is a common task, shared between the EU and the member states. It would be helpful to get some idea of how this responsibility is split between the EU at the centre and the member states. What is delegated and what is shared? Andrea, can you just give a picture of how the whole thing fits together?

Andrea Garcia Rodríguez: I first want to add a couple of figures to illustrate what Markko was saying when it comes to the EU. I mentioned that one reason why we are seeing more online fraud is that people are using e-commerce more often, especially since the pandemic. I have some figures that will help us understand the scope of the problem. In 2015, only 7% of European SMEs sold their products through other European countries. In 2019, before the pandemic, the figure had doubled to over 15%, but trust among online users has decreased. In 2015, it was 38%. During the pandemic, it rose because more people were doing their purchases online, but it has not kept up with the increase in online purchases.

As an example, the people who buy most online are young people, which brings me back to online education. Of the things that people between 15 and 24 years old bought, 80% were bought online. That is a key point when we think about this.

On your question about how the EU is sharing responsibility for dealing with online fraud, Lord Young, as I mentioned, the EU is trying to put forward a new set of rules that would help us fight this. Specifically, I mentioned the Digital Services Act, under which the responsibility will fall first on online platforms, in collaboration with different figures, such as the newly created trusted flaggers, who will try to spot illegal content. These trusted flaggers are associations that have a track record in identifying and reporting illegal content online. These entities will work with platforms to say, "Hey, we've spotted these online ads that lead nowhere and this is fraud". They will collaborate with the platforms to remove that content as soon as possible.

Then it will be the responsibility of the European Union and national entities for the oversight of these platforms, depending on the size. If they are very large online platforms—or VLOPs—which is the name that this piece of legislation uses for platforms that have more than 45 million active users, or 10% of the European population when it comes to active users, it will be the European Union strictly enforcing this regulation or doing this oversight. If it is less than that, it will be the member states, so it would be more or less a shared responsibility. It is a common endeavour.

Lord Young of Cookham: Can I just ask a question about Europol, which is the law enforcement agency? When the UK left the EU, we stopped being members, but we were entitled to apply for third-country status. I wonder whether you know how those negotiations are getting on, so that we get as many benefits from having access to Europol as is possible within the confines of Brexit?

Andrea Garcia Rodríguez: I cannot comment on that. I have no idea.

Lord Young of Cookham: Perhaps you could drop us a line if somebody has the answer as to what the relationship now is between Europol and the UK.

Q175 **The Chair:** I had a question for Markko. I understand that Estonia had a key role in developing the National Cyber Security Index, where Estonia currently sits third, and NATO's Cooperative Cyber Defence Centre of Excellence, which is based in Tallinn. I wondered whether there were any learnings from their work in relation to digital fraud and cybercrime that are particularly relevant to this committee?

Markko Künnapu: We started several years ago with the National Cyber Security Index, which was developed by the Estonian e-Governance Academy. We still have it, and it can be considered a very useful tool to compare ourselves with other countries as to where we stand and what the problems and challenges are. Also, other countries can learn from that.

Although the title is "cyber security index", we have taken a very broad, holistic approach and we also address criminal justice-related issues. How is the country dealing with cybercrime? What is the state of play regarding cybercrime legislation? Does the country have in place a dedicated cybercrime and digital forensics unit? Is the country part of international instruments such as the Council of Europe Convention on Cybercrime? What international co-operation networks is the country party to and using?

Therefore, it is a very useful tool. We have learned a lot about how other countries are doing and where we stand when compared with them. This index and its results are being used for capacity-building project purposes. In cybercrime and computer-related fraud, we are dealing with cross-border crime and we need to co-operate with other countries as much as possible. If a country has problems with legislation or capacity, these indexes and their results can be used to provide assistance.

Co-operation with the NATO Cooperative Cyber Defence Centre of Excellence is a bit different, because it is part of the NATO organisational framework. However, we also have very good co-operation with it. It does a lot of work, in particular different reports and studies on the cyberthreat landscape, the cybersecurity situation and cybersecurity strategies all over the world. We can benefit from this same information.

What is also useful is the training that the centre provides. Its cybersecurity exercises are open to government authorities. This is the benefit that we have gained from this—more information on what is happening and all these practical measures, such as training and joint cybersecurity exercises, which often involve other NATO countries and other organisations.

The Chair: Does NATO share any intelligence? We have heard evidence that behind a lot of fraud that affects individuals sit criminal gangs, which are engaging in money laundering or financing of criminal activities. Is there a sharing of intelligence through those bodies, or is it done, as Lord Young was suggesting, more through Europol or other international law enforcement?

Markko Künnapu: We are talking here about different frameworks. They are more involved in the military use of cyberspace information and operations, and maybe cyber-related espionage. When it comes to the fight against fraud and cybercrime, this is the responsibility of member state law enforcement authorities, using Europol, as a facilitator or hub for information exchange, and Interpol, to co-operate with and reach other countries.

The Chair: Andrea, I can see you are nodding. A lot of fraud is cross-border. It would be helpful to hear your comments on how the different law enforcement agencies across Europe share information, particularly on criminal gangs. Also, with the UK now having left the EU, we are now relying on mutual legal assistance treaties. Do you have anything to say on how well those treaties work in the digital age?

Andrea Garcia Rodríguez: We forgot to mention something really important when it comes to prosecuting fraud, which is collaboration with the private sector. That is also key. As Markko said, and why I was nodding the whole time, NATO is a great platform to share intelligence when it comes to military activities and the type of cyber criminality that would impact the military power of allied nations. Interpol and Europol are fora to exchange information about different types of cybercrime activities, but what we are missing here is precisely this picture.

To refer to a specific example, during the first weeks of the Russian invasion of Ukraine, Microsoft put forward a very comprehensive report about the cyber trends that it was seeing, because most people use Microsoft and Windows OS. Therefore, it was able to get more information about the targets and the trends, and it did a fantastic report that was very helpful for policymakers not only in the EU but in national states. That is really important.

We are seeing how multistakeholder governance and co-operation can help us to fill the intelligence gaps that we sometimes have as member states when we collaborate through other fora, precisely because the collaboration frameworks of these fora are very strict and the scope is very well defined. I would like to add this new piece to the conversation, because it is very relevant for tackling online fraud.

The Chair: This is very helpful. Markko, from the Ministry of Justice in Estonia, do you have a view on the best way for Estonia, for example, to co-operate with a non-EU country in chasing a criminal gang related to fraud? Is there something that has particularly worked?

Markko Künnapu: As cybercrime is cross-border most of the time, one country has to co-operate and exchange information with other countries, and often with third countries that are not member states of the European Union. There are different possibilities for this, such as police-to-police co-operation. Countries that are state parties to the Council of Europe Convention on Cybercrime, the so-called Budapest convention, can easily use a 24/7 network and points of contact, which are in place in involved state parties and can be used to send information on a spontaneous basis or to request the preservation or production of data.

There are also channels available that have been provided by Interpol. There are some other treaties, conventions and protocols that can be used, but again there is a need to co-operate. We need to find additional ways and means to make this co-operation faster and more effective. Right now, when it comes to investigations of fraud or other types of cybercrime, computer data that is needed and could be considered as electronic evidence is, most of the time, stored somewhere abroad. Then you need to co-operate with other countries and with the multinational service providers that hold the data.

Q176 **Viscount Colville of Culross:** Andrea, you have talked about the Digital Services Act requiring these very large platforms to do risk assessments on the conduct of illegal activities, including the sale of counterfeit products, and how that will be enforced at an EU level to stop counterfeit goods. How will that enforcement take place? You also said that thousands of smaller platforms will be looked at by the national police. Will there be a difference of standard in stopping the sale and advertising of counterfeit goods for these smaller platforms across the EU?

Andrea Garcia Rodríguez: On the last point, co-operation is key. It is important to develop a single point of contact for consumers when they experience fraud and for national states and different bodies. That will be really useful, to answer your question.

On enforcement, unfortunately that tends to be the big question when it comes to EU regulation. The European Union is very ambitious, but enforcement tends to be the keyword to make it happen. We saw before with different pieces of legislation, such as the GDPR, that enforcement fell on the national authority of the country. Most platforms are based in Ireland, so the Irish authority is overwhelmed and therefore cannot enforce GDPR in the way it should. There is always lots of delay because of that.

Unfortunately, I think the DSA will go the same way. I mentioned that there are a few means of enforcement, because it is the commission that identifies VLOPs. It would not be the national authorities doing so, but the commission that would put forward the list of these very big platforms. Right now, it is estimated that there would be around 35. By the time that these are put into place in January 2024, we would probably be thinking about 50 different companies that would make it to the list, but there are plenty of other online platforms.

That is why, when it comes to enforcing the DSA for very large online platforms and search engines, it would be the European Union and the Commission, while for the rest of the platforms it would be the national authorities. It does not mean that it would be the national police. The police would barely need to do anything. Here, it is the specific authority that has been created in the different member states that would serve as this single point of contact for consumers and for the Commission when it comes to enforcing the the DSA and the DMA.

Viscount Colville of Culross: You had problems enforcing the GDPR, so are there any lessons that can be used for trying to enforce the DSA? You said that there was going to be a single point in each nation for trying to deal with these smaller platforms. Does that not mean that you will not have a uniformity of requirement or of enforcement against counterfeit goods on these smaller platforms?

Andrea Garcia Rodríguez: There is a difference between the governance structures of the DSA and the DMA, and the way they will be enforced in prosecuting these online crimes. I am talking specifically about the governance, because the problem with VLOPs is that they monopolise most of the services online and therefore require greater oversight than smaller platforms. We are speaking about the 35 to 50 very large online platforms that will have to do specific things to ensure that the products placed on these platforms are safe to use and licit. That is the reason I was referring to those.

It does not mean that that is not going to be harmonised; it is, but in other pieces of legislation. It is a multilevel structure of governance, so oversight of the biggest will be by the Commission, which will have more powers to do more direct enforcement, whereas the others that are supposed to handle less information and fewer products will be overseen directly by member states.

One lesson that we could learn for the future is that decentralised government is very helpful in this regard, because you can avoid the concentration of actions with a single body. I refer specifically to the GDPR and to Ireland, because that is a very clear case of how we could have avoided that. For example, if Google had its headquarters in Greece instead of in Ireland, that would help us prosecute what is doing in a different way, because we would be able to have more resources. The problem is always the amount of resource available, such as people devoted to the enforcement of this legislation, time and many others.

Viscount Colville of Culross: Markko, are you concerned about the enforcement of the DSA when it comes to counterfeit goods that are on the very large platforms?

Markko Künnapu: The main issue here is that these are legislative Acts, not criminal justice instruments. Their objective is to protect customers. Service providers will have certain obligations concerning actions that they need to take in case illegal content related to crime or fraud is detected, as well as obligations to notify domestic law enforcement authorities. This would be quite useful. Definitely, co-operation between service providers and law enforcement would improve. Pursuant to these new Acts, service providers have must not observe or monitor the data that is being processed. In the case that they detect illegal content, these obligations need to be fulfilled.

They need to react if other individuals or competent authorities notify them that they are hosting content that is considered illegal or is related to crime. These new Acts will not eradicate cybercrime, but they will definitely make co-operation between the private sector and law enforcement easier and more effective.

Viscount Colville of Culross: Markko, are you concerned that the smaller platforms could be held to a different standard when it comes to dealing with fraud than these very large platforms?

Markko Künnapu: Yes, because the situation could change and criminals could move from larger to smaller platforms. This forum shopping is not new. There is a serious concern that smaller platforms could be exploited by criminals in the future.

Viscount Colville of Culross: What needs to be done to prevent that?

Markko Künnapu: Again, it is closer operation between law enforcement and these smaller providers. If smaller providers realise that they could be abused and their services exploited for criminal purposes, they should pay attention to this and take necessary measures on how to avoid these kinds of situations.

Q177 **Lord Sandhurst:** Markko, I have a question with three interlinked parts, although not very complex. I think that EU Governments will be able to request the removal of illegal content that promotes commercial scams. Is that right?

Markko Künnapu: Yes. If a website or server is hosting content related to the commission of crime or information that is being used by criminals to commit those crimes, yes, the authorities can contact this particular provider, and this illegal content or information needs to be removed.

Lord Sandhurst: Will that extend, effectively, in two ways? These are the second and third questions. First, will Amazon or other online marketplaces have to implement systems to take down advertisements for counterfeit products, in other words? Do you see where I am going?

Markko Künnapu: Yes, this should be the case, but they are not monitoring in real time what is happening, what is being offered or what is being sold. In the case of notification, they should react to this and block or take this content down.

Lord Sandhurst: So you would like them to do that. Should there then, following this up, not be an obligation on the platforms, such as Amazon, to know their advertiser? Their primary obligation is then to prevent it.

Markko Künnapu: It is not very easy to answer this question. Very large providers have thousands or millions of customers. When we talk about Amazon, there is also Amazon Marketplace, which individuals can use to sell goods. Know your customer measures should be in place to prevent fraud.

Lord Sandhurst: The advertiser is not the customer.

Markko Künnapu: They are also a kind of customer.

Lord Sandhurst: It depends, yes. It is the advertiser who is bringing someone in.

Markko Künnapu: They should make sure that platforms are not used for the kinds of activities that would facilitate or promote fraud.

Andrea Garcia Rodríguez: There is a very clear answer to that. Under the Digital Services Act, specifically Article 24, every time an ad is displayed to somebody, there are three things that that piece of advertising should comply with. First, it should clearly show that it is an ad. Secondly, it has to show on behalf of whom this ad is being displayed—the specific company or person who put it on the market. Thirdly, it has to clearly show why you have been targeted with that ad. It has to show information about the parameters for the ad personalisation algorithm that made that ad reach your computer specifically.

There are these clear transparency obligations now under the DSA, which means that, in the case of fraud, you have to be able to identify who put that ad out there, for what purpose and who that ad wanted to target. You should then have the mechanisms to pull that down if it shows that it is not licit content.

Lord Sandhurst: As a follow-up, if the advertiser is not doing that or the platform is not preventing the advertisements coming up, what remedies are there on the part of the Government or the regulator to deal with that after the event?

Andrea Garcia Rodríguez: If I am not mistaken, where the platform does not do it sufficiently quickly, it could face a fine of up to 10% of its global revenue, so there is that incentive to identify it. As Markko said, there is this figure of trusted flagger who can say, "Hey, this has happened. You should remove this ad. If you don't do it in a sufficiently quick manner, you can be fined up to 10% of your global revenue", which is a lot. Fines could definitely be bigger than we have seen before in Europe.

Lord Sandhurst: If we wanted to come back to you for follow-up or for a bit more detail on that, could we do that in private session?

Andrea Garcia Rodríguez: Yes, we could, for sure.

Lord Sandhurst: Estonia has introduced some new measures to deal with cryptocurrency. What are you doing with that, Markko? Then, for Andrea, how will the crypto assets regulations be applied in the EU?

Markko Künnapu: In Estonia, there have been several recent legislative amendments related to crypto assets and these virtual asset service providers, but most of them were related to the fight against money laundering and prevention of financing of terrorism. That means additional obligations to those service providers that they should know their customers and conduct due diligence—similar obligations to those that financial institutions have. Not only ordinary individuals but criminals often use these services to move large amounts of money from one jurisdiction to another.

Cryptos are often part of digital or computer-related fraud schemes. There are different real, but unfortunately also fraudulent, trading places and crypto exchanges, and often victims are invited to these platforms. They present the expected profits, and people transfer money and invest in these schemes, crypto coins and assets, but in real life they just lose all their investment.

We have also seen cases of ordinary fraud where people lose money, it is transferred from one account to another, and it is converted into crypto assets in order to make tracing difficult or even impossible. This is why, again, co-operation with these providers is an important response, and why they need to have certain obligations and responsibilities towards their customers. They are also expected to co-operate with law enforcement authorities in cases where their services have been used for criminal purposes or have been part of these criminal schemes.

Lord Sandhurst: Andrea, did you have anything on crypto assets?

Andrea Garcia Rodríguez: This is not my area of expertise, so I cannot give a very long speech about how the EU is dealing with crypto assets, but there are a couple of things that I would like to mention.

First, there is a proposal for a regulation that we are currently working on, the MICA regulation, which stands for markets in crypto assets regulation. Specifically, it seeks to create new parameters and areas of transparency for crypto intermediaries, and to create a minimum requirement for crypto assets to be launched in one of the trading platforms. For this, if I am not mistaken—I will probably need to check—the company that wanted to issue a token through these online platforms had to have minimum capital to do so.

Secondly, the most interesting thing in this regard, and we are debating this in Europe, is that, as of now, while people trade in this type of assets, they do it through intermediary services such as Coinbase, Binance and KuCoin. Would these specific places be subject to the DMA and the DSA? That is an open question. This is not an answer, but that gives us a picture of how complex this is. We are specifically speaking about tokens with the specific characteristics that they play in a non-transparent way. The EU is trying to create transparency provisions to do so, but these items are normally traded using intermediary services that we are not yet sure should be included in the DMA and the DSA. We will decide in the near future whether they should, but it is an interesting conversation that I would like to follow up after this.

Q178 **Baroness Taylor of Bolton:** It has been very interesting hearing so many similarities about the problems that you are facing. We have talked about international co-operation here quite a bit. Clearly, there is not one silver bullet. You have mentioned various things such as intelligence sharing and joint exercises. What is the main barrier to successful international co-operation within Europe, the UK or, indeed, globally? Although there will not be a silver bullet, what would be your one priority in any new measures that could be taken to improve the global effort against international fraudsters? They do not know any international barriers, yet the institutions that are dealing with them clearly have to. Andrea, you were nodding thoughtfully there.

Andrea Garcia Rodríguez: Markko can go ahead. I was trying to gather my thoughts.

Markko Künnapu: The biggest challenge right now is that, most of the time, cybercrime and computer-related fraud are cross-border. That means that victims, perpetrators and electronic evidence that is needed to investigate a case can also be in different jurisdictions. The classic mutual legal assistance treaties might not be sufficient for this, because the amount of bureaucracy that needs to be fulfilled can be quite slow and often ineffective. By the time a mutual legal assistance request is sent, it could be the case that the data that is needed—IP addresses or traffic data—is not there anymore. The data has been deleted or destroyed. If law enforcement cannot access the data, it cannot continue with the investigation.

Therefore, the biggest challenge is to ensure that data is available and that co-operation is faster and more effective, in order to improve the solutions that have been developed. For example, the Council of Europe recently adopted and opened for signature the second additional protocol to the Convention on Cybercrime, which would provide additional tools for law enforcement to use in parallel with the classic mutual legal assistance mechanisms.

The European Union has been discussing, for quite a few years already, how to improve access to electronic evidence and how to make co-operation between law enforcement authorities and service providers more effective. So far, there is no agreement with the European Union, but the second additional protocol to the Convention on Cybercrime is already there. I hope that states will ratify and start using this in practice.

These are the biggest challenges and concerns right now—how to ensure that data will stay until needed, and how to ensure quick and effective access to this particular data.

Baroness Taylor of Bolton: As consumers, we have got used to doing everything instantly. Maybe we need to think about slowing down the process when we are doing our internet banking or, indeed, shopping online. The speed of the authorities checking things does not match what the fraudsters can get, by the sounds of it.

Andrea Garcia Rodríguez: It is also relevant, as I mentioned, to collaborate with the private sector and to attract third countries through the efforts that the UK and the EU are making in fighting cybercrime. As Markko said, if we go back to the Budapest Convention on Cybercrime, we can see that only around 70 countries signed it. The convention sought to harmonise the legal frameworks of the signatory countries, so that, if you found a perpetrator in one of these countries, you could legally prosecute them.

The problem with that is that most of the 70 countries are western countries. The big countries that we would know as being the origins of these types of cybercrimes—China, increasingly, or India and others—never signed the convention. The problem we have nowadays is that, as Markko mentioned, because of the global nature of cybercrime, you need to co-operate globally to tackle it effectively. I would see this happen in three layers.

The first would be at home, not only trying to create a stronger balance between the police and the Government, but including regional and city governments in this, because the more information you have available, the easier it will be for you to spot these cybercriminals before they act.

The second thing would be stronger co-operation regionally, between the UK and the EU, but also the United States. I am thinking of specific fora which, because it is no longer part of the European Union, the UK does not participate in, one of them being the TTC—the Trade and Technology Council—which is becoming so important. We have seen it ever since 24 February and the Russian invasion of Ukraine.

The third thing would be using this very strong co-operation in forums such as the United Nations—Markko knows this very well, being in Vienna at the moment—and in collaboration with third countries. We are seeing this as part of the digital partnerships that the EU is doing with countries such as Japan. That is the one that I can think of at the moment, because the joint statement was recently released, but I am also thinking of countries in the Middle East. The UK could use its advantageous relationship with India and other countries that the EU is perhaps not so keen on collaborating with, or that we have different ties with. Bringing together a more diverse pool of actors can definitely be the way out of this, because the UK and the EU have very strong ties, but we are only 10% of the global population, so we need to keep working on that.

Baroness Taylor of Bolton: That is a bit depressing, but thank you.

The Chair: Thank you very much indeed. We are very grateful to you both, Markko and Andrea, for joining us for this session. I suspect that we could have asked you lots more questions, but thank you for logging on this afternoon and for sharing your expertise.