8th IAP Eastern European and Central Asian Regional Conference

„Asset Recovery and Cybercrime“

2017 June 26-28

Jurisdictional issues related to assets in e-currency – Austrian perspective

Ladies and gentlemen, dear colleagues,

I feel truly honored for the opportunity to hold a speech in the presence of such a high-level circle of colleagues about the Austrian perspective of jurisdictional aspects related to the quite new but highly current phenomenon of e-currencies or – to be more precise – of virtual-currencies.

When virtual-currencies appeared not even a decade ago, the criminal society recognized immediately, that this development opens a large field for criminal action and criminals learned very quickly how to use these new opportunities.
In contrast to that, the public authorities underestimated this phenomenon totally for quite a long time. So legal experts in the fields of teaching, the making and the practical application of laws in Austria (as well as in many other countries) are just at the beginning of discussing the various issues related to virtual currencies and there are still many aspects to be solved.
As we are talking about an international phenomenon, which is not bound to any national borders and sometimes not even relatable to a specific geographic location, one of the crucial issues – beside the legal situation of criminal procedure and international co-operation – is also the field of jurisdictional aspects; in other words the issue, which state is responsible to take action in a case related to virtual currencies and in relation to the recovery of assets in virtual currencies or under which circumstances declares a concrete state his law enforcing authorities competent to do so.

Of course as a basis for a legal analysis in this context it is – first of all – absolutely necessary to understand the nature of virtual currencies like Bitcoins (and many others) and to pay attention to their characteristics.

Therefore I first would like to give you a quick **portrait of virtual currencies** by the example of Bitcoins in a nutshell, just by outlining their **basic** (somehow also technical) **characteristics**, but without going to much into technical details:

The idea for inventing virtual currencies resulted from the fact, that commerce on the internet relied mainly on financial institutions serving as trusted third parties to process electronic payments, which was considered as slowly, costly and – due to the reversibility of transactions – as uncertain.
The aim was to create a **webbased electronic payment system**, which accomplishes all functions of traditional money, but which ensures **immediate and irreversible transactions** at low price and enables **direct transactions** between two willing parties by using a **peer to peer** distributed network and an **automatically generated cpryptographic proof**. This concept led to the Bitcoin-system, which still is the most used virtual currency.
Bitcoins **do not consist of physical entities**, like coins or banknotes. Bitcoins are **only** electronical accounting units, they exist only as **electronic data**, generated and administered automatically by a decentralized peer-to-peer network, which consists of all devices, where the Bitcoin-software (client) is installed.
So there is **no central institution**, no central bank, which issues this currency, and no central institution, which could exercise control over the relating transactions or which could be an addressee for public authorities in criminal proceedings.

The **value** of Bitcoins is not covered by any real goods (like gold) or ensured by a government; it is based only on the belief of all participants of the system in the integrity and security of the decentralized network and **depends only on the supply and demand** of the network. It is therefore highly volatile.

Electronic **transactions** of Bitcoins work quite similar to a bank transfer but **use cryptographic keys** (a public key serving as an address or account number and a private key) instead of names or e-mail-adresses, which makes the Bitcoin-system most widely **anonymous**.

Each electronic transaction is disclosed and released to the network, which verifies and stores it by using the so called **blockchain-technology**. This technology is a **constantly growing bookkeeping** of all (electronic) Bitcoin-transactions ever made since its creation based on a special (for mortal individuals miraculous) algorithm, which is **practically unchangeable** in the aftermath and avoids therefore double spending.
This blockchain is updated every few minutes. The actual version of it is permanently **distributed to the whole network**, in other words to every member of the network, so that all electronic transactions are visible for every participant. But as the keys are kept **anonymous** it is almost impossible to link these transactions to the person behind it. It is obvious that this anonymity is the crucial incentive for criminals to use virtual currencies like Bitcoins.

Trading of Bitcoins happens either between private persons directly (by an **electronic transfer** of a certain amount of Bitcoins from one address to the other or just by **handing over the relevant keys physically**) or at **trading platforms**, where you can also **change your bitcoins into traditional currencies**.

If you own Bitcoins, you store them by using "**wallets**", a software, which **stores just the relevant keys** and which is offered by **various providers**.
As Bitcoins are just electronic data, wallets can be kept in **every kind of electronical device** (USB-Stick, Smartphone or PC) or **just online**.
Of course these files can be backed up like every other file, so that the relevant keys, which grant access to your Bitcoin-assets, can be located at various places concurrently, also as a **hardcopy version (paper wallet)**.

Every person who gets access to the relevant keys has automatically unlimited access to the related assets of Bitcoins. If the **keys are lost**, this practically also means the irrecoverable **loss of the related Bitcoins**.

The legal nature of bitcoins is still subject to discussions. It is obvious that bitcoins cannot be seen as an **object**. They also do not fulfil the requirements of being a specific **right** or title, because they do not give the owner any legal position against a third person.
But they are – in our understanding – **data in the sense of penal law** and they fulfil the requirements to be seen as an **economic value**.

So – to repeat that – if we speak about e-currencies or virtual currencies like Bitcoins, we speak of **unregulated digital money**; a digital representation of value, which is **not issued by a central bank**, credit institution or e-money institution, but **issued decentralized (or even automatically**) **beyond the control of public authorities**, sometimes based on cryptographic algorithms (like Bitcoins). Values in these currencies are only **stored electronically** and the **essential keys** to get access to them can be stored in various copies on any kind of device (Smartphone, PC, USB-Stick) or at any other place in the internet (cloud, custodial wallet provider). By doing that, various **encryption methods** are used, which make it almost impossible or at least very **difficult to link such assets or correspondent transactions to identified individual persons**.

For the legal part of my presentation I would like to begin with a short overview of the legal situation in Austria concerning confiscation and **forfeiture and our jurisdictional approach** in general as well as towards assets related to criminal acts and penal cases.

Basically we could say, that Austria is highly interested to withdraw effectively any assets, which are generated through criminal acts respectively assets associated with the criminal sphere or society.

Due to international guidelines and requirements (like directives from the EU) or recommendations (like GRECO, FATF [Financial Action Task Force]) Austria has amended its legal provisions on confiscation and forfeiture at the beginning of 2011 in order to widen the possibilities to get access to illegal assets.

In principle now **any kind of assets**, which are **acquired for or through an offence**, are to be forfeited to the court.

Forfeiture also **extends to any benefits and replacement value** of such assets, like **interest, increase in value** or items, which were financed by such assets.

Generally these provisions do not only hit assets, which are in possession of a perpetrator, but **also assets belonging to third persons**, unless these persons purchased these assets whilst unaware of the offence.

Also assets that are in the possession of a **criminal organization or a terrorist group** or that have been collected or provided for the financing of terrorism are to be forfeited.

Even assets, which were acquired only **in a temporal connection with an offence** are to be forfeited, if there is reason to believe that they also were acquired by a criminal act and if their **lawful acquisition cannot be substantiated**.

As a basic principle these provisions **affect all assets**, no matter if they are located **in Austria or abroad**, as long as the relating criminal act itself comes under the jurisdiction of Austrian criminal law.

This basically is the case, if the criminal act itself was **committed in Austria** (territorial principle), which means that the perpetrator has set at least a part of his relating criminal **action in our country** or if a **result element** of the offence, in whole or in part, occurred or should have occurred **in our country**.

Beyond that, the jurisdiction of Austrian criminal law is also given in relation to criminal acts committed outside of Austria, if national interests are concerned (e.g. narcotic drugs trafficking or money laundering in relation to offences committed in

Austria), if the perpetrator cannot be extradited or if Austria – due to international obligations – is bound to do so.

Further on, the provisions on forfeiture also extend to **assets located in Austria** in relation to **offences, which do not come under the jurisdiction of Austrian criminal law** themselves, but which are punishable under the laws of the place where they occurred.
In this regard – as an example – assets of international criminal organizations could be declared forfeited, even if the organization itself did not carry out any criminal action in Austria.
In this context the term "Located in Austria" – of course – means, that items have to be in Austria physically. If we talk about a bank deposit, this deposit must exist at an Austrian credit or financial institution.

As a precondition for a court´s decision pronouncing forfeiture the affected assets have to be recovered by the police respectively by the public prosecution service or seized by an earlier decision of the court in the pretrial-phase.
Unless such assets are recovered or seized the court has to forfeit a monetary equivalent.

Beside the forfeiture the court can also confiscate any item used or intended to be used in the commission of an intentional offence and any item (or replacement value) yielded from such an offence, if it belongs to the perpetrator.

To summarize that, we can say, that the Austrian provisions on forfeiture are quite rigorous and severe and that our jurisdictional rules allows a widespread application of Austrian criminal law:
If a criminal act comes under the jurisdiction of Austrian criminal law, Austrian jurisdiction covers also the decision about relating assets, wherever they are located (in Austria as well as abroad).

If a criminal act does not come under the jurisdiction of Austrian criminal law, Austrian authorities nevertheless have jurisdiction to decide upon all assets related to this (foreign) criminal act, as long as these assets are located in Austria.

Of course the execution of such an Austrian decision upon forfeiture or seizure (or a recovery order of the public prosecution service) related to assets, which are located abroad, is another story. But this is not a jurisdictional issue but an issue of the effectiveness of mutual legal assistance and international co-operation.

To illustrate the Austrian jurisdictional approach let me give you a few examples:
.) Let us suppose, a person uses the internet in his home in Austria to blackmail somebody in another country by e-mail.
Due to the territorial principle this case would come under the jurisdiction of Austrian criminal law, because the **perpetrator acted in Austria**.
.) If it is the other way round and a person uses the internet in a location abroad to blackmail a person in Austria, the case would also come under Austrian jurisdiction, because the **result of the offence occurred in Austria**.
In both cases the Austrian court would also have to decide upon all assets related to this case, no matter if they are located in Austria or abroad.

.) The third example shows our jurisdictional limits related to internet-cases:
A person living in Hungary detected that somebody **misused** the **data** of his credit card (the card itself was not stolen) to **purchase something online** on the internet by using the **website of an Austrian Company**. As a result the victim´s bank account in Hungary was debited with a certain amount of money.
The Austrian authorities **denied the application of Austrian criminal law** in this case, because there was **no evidence** or suspicion that the **perpetrator himself acted physically within Austrian territory** and because the **result of the offence** – the damage of the victim – **occurred outside of Austria**, in the concrete case in Hungary. The use of a website of an Austrian Company was not seen as the place of action (by

the way it is not necessarily the case, that a website is hosted and therefore located at the same place as the corresponding company).

Nevertheless an Austrian court in this case would have jurisdiction in regard to a decision of forfeiture of **assets located in Austria** related to this case, for example if the perpetrator used the stolen data to purchase some kind of electronic assets or credits, which are administered by the mentioned Austrian Company.

Another issue, which becomes imminent in many cybercrime related cases and which also implicates some jurisdictional aspects is the question, if a state is allowed to carry out **criminal investigations directly in another state by using a trans-border access to stored data in the other state**.

This is still an **ongoing discussion** in the EU. But so far we have to respect the **limits given by the convention on cybercrime of 2001**, which allows such trans-border activities only in view of **open source stored computer data**, or if the **lawful and voluntary consent of the affected person** (the person, who has the lawful authority to disclose the data through the related computer system) is obtained.

This means, that if these requirements are not fulfilled, we still have to use the existing channels and **instruments of judicial co-operation**.

Coming back to **Bitcoins** or other virtual currencies we have to point out that stored values in such currencies are seen as assets in the sense of the described provisions and that they could therefore – as well as any benefits and replacement value of such assets, like interest or increase in value – be a subject matter of a Austrian court´s decision on **forfeiture or seizure under the same conditions as any other kind of assets**.

But if the positive affirmation of jurisdiction of Austrian authorities or the execution of a decision of an Austrian court on forfeiture or seizure relating to assets depends on

the geographical **location of these assets**, we have to face a quite uncommon situation as soon as it comes to virtual currencies:

This first of all is the case, because virtual currencies only exist as immaterial sets of electronic data, which habitually implicates at least some investigation efforts to find out the exact place of storage.

But if we speak about virtual currencies like Bitcoins, this situation gets even worse, as the use of the mentioned blockchain-technology (in other words, the fact that the relating data is distributed worldwide automatically to every single member of the network) consequently leads to the conclusion, that assets in Bitcoins simply are located almost all over the planet.

Deducing jurisdiction only from the fact, that "all over the planet" logically means "also in Austria", would create a kind of universal jurisdiction related to assets in virtual currencies. Such an approach would be unfunctional and simply too wide in our understanding.

It makes much more sense to **stick to the geographical location of the relevant keys** or wallets as far as possible. Such an approach is still wide enough, but it is – at least to some extent – more specific than an universal jurisdictional approach based on the **ubiquity of the blockchain**.

So if the relevant keys respectively the wallets are stored on a physical **device (mobile phone, PC etc)** or exist in any other way **physically** (like paper wallets, where the keys are just printed out), we would consider the relating assets themselves as being located in Austria, if this device or item is located in Austria, even if various backed up copies exist in any other kind of appearance somewhere else.

If a **wallet** is used, which is relatable to a concrete provider or company, we would – in analogy to bank accounts – assume the relating assets as being located in Austria, if the mentioned **provider is seated in Austria**.

The same procedure would apply in relation to wallets in a cloud, if it is technically possible to link them to a concrete provider.

The subsequent question, if the addressed provider then will technically be able to freeze the wallet and/or to grant access to it, is – again – another story, but does not concern the jurisdictional issue.

To sum up, I can say that in view of criminal cases related to assets in virtual currencies, it will be an enormous effort for the experts in the making and practical application of the law of our countries to find practicable answers to all the different **issues, which will come up** in the very near future in this context or which already are on the table, waiting for an appropriate solution.

But in my view, most of these issues are not related to jurisdictional aspects; they will mainly concern other topics:
One of them will affect the **technical level**, where we have to prepare the ground and explore all options for effective criminal investigations on a technical basis.
Another area will be the **finding of new legal instruments** or the adjustment of existing instruments in the **fields of criminal procedure and international cooperation**, because these instrumens should be appropriate to the technical characteristics of the new phenomenon of virtual currencies and their corresponding consequences (like anonymity).

Based on the shown Austrian perspective, **jurisdictional issues** play only a minor dramatic role in comparison to the previous mentioned issues, because also under the given provisions there is only very little space, where crime related assets could be – from a jurisdictional point of view – considered by criminals as being in a safe haven.
But if it comes to the discussion on the power to directly carry out **online-investigations in other countries** compared with the use of traditional instruments of judicial co-operation, the international community still has some work to do. Because in this regard we are talking about the effectiveness of criminal investigations respectively about speed, and speed is one of the crucial points, when we try to recover crime related assets, which are stored electronically.

Thank you very much for your kind attention!

Contact details:
Michael Leitner
Deputy Prosecutor General
Procurator General´s Office - Generalprokuratur
Schmerlingplatz 11
1010 Vienna
Austria
+43 1 52152-3405
michael.leitner@justiz.gv.at