COPENHAGEN LEGAL TECH LAB — PODCAST

EPISODE 08 – CYBERSECURITY: DENY, DENY, DENY

In this episode, Alexandra Andhov, Associate Professor at the Faculty of Law, University of Copenhagen and founder of the Copenhagen Legal Tech Lab, and Luigi Bruno, Privacy Engineering Leader and Cybersecurity and Privacy Leader for Investments in Group Digital at IKEA, discuss the topic of Cybersecurity arguing how and why this matter should be relevant to lawyers.

00:00:00
Intro music

00:00:07,940
Alexandra Andhov
Hello and welcome to the Copenhagen Legal Tag Lab podcast, where we address innovation and the law from three angles people, technology and business.
My name is Alexandra Andhov, and today we are at the Law, Innovation and Vulnerability Conference at the Faculty of Law at the University of Copenhagen. Together with Luigi Bruno, a privacy engineer, leader and cybersecurity and privacy leader for investments at Ikea Digital.
Luigi is a lawyer and a computer scientist, and he is also completing his PhD at McGill University in Canada. So, hi. Welcome Luigi.

00:00:50,729
Luigi Bruno
Hi. Thank you so much for having me. It's a pleasure.

00:01:01,810
Alexandra Andhov
So, during the conference on Law, innovation, and vulnerability, we have a panel on cybersecurity that is called “Cybersecurity. Deny, deny, deny”. And that somehow comes from my previous experiences working predominantly with financial investment companies that, if anything, of cyber breach security concern happened, they did not necessarily want to disclose it too much.
So that's maybe something that my background is in, but I do think that and the reason why we brought this topic to the conference is that we believe, and we are very happy that you agreed to do this podcast with us, is that cybersecurity should be truly in everyone's concerned, right?

Because of how digitize our world is and how much data is out there. A lot of personal data, a lot of really private data. We should be aware of what are the risks and how do we minimise these risks if something happened to this data. And the purpose of today's ultimately podcas is really to understand what is cyber security and how and why is cybersecurity relevant for a lawyer?
So, maybe let's start with the first question. So, what is cyber security?

00:02:34,280
Luigi Bruno
That's a million-dollar question. So, last year I had a chance of teaching a course called Cybersecurity for lawyers and Miguel and, you know, before approaching that course when I was designing it, I was actually asking myself the question. If I take out my computer science background and my, you know, professional experience, how as lawyer I would like to hear about cyber security. So, I think if I take that angle now, maybe for the audience, if there's many lawyers listening to us, there might be useful.
I think let's start with the definition because as a lawyer, I think it's always important to have a definition that we can hang out there. So, the definition that you can find on books is like so cyber security is basically the protection of the assets of a computer system. So, what are these assets? Right? The assets are hardware. So, think about, for instance, your CPU or your screen or anything that's like tangible. Then you have software which think about, I don't know, Windows operating system, Mac operating system, anything that's intangible. And then you have data. Now I'm not gonna say data it's tangible or intangible. There's a debate out there. Some say it's tangible. Some say it's intangible, but that we can talk about it another time.
Now, having sort of framed this a little bit, I think the next step is to understand a little bit of basic terminology, because when we hear about cybersecurity or we read about cybersecurity, non-specialised magazine, there's a lot of buzz words that are thrown around right, so we hear about threat, vulnerability and risk and attacks and hackers and, you know, cyber warfare and all these things. But let's try to sort of, like, do a little bit of a lexicon or which are the most important terms to just know and dispel a couple of myths.
So, what's a vulnerability, right? I mean, if you think about the word vulnerability that makes you think about something that can be exploited. So essentially, it’s a weakness in the system, so it can be a weakness in hardware and software or a weakness in how you manage your data. Then we have a threat. So, a threat is, you know, something that you know might happen. And so, the threat is especially, let's call it the set of circumstances that someone might exploit a vulnerability to cause you harm.

00:04:51,920

Alexandra Andhov

Okay, and could you maybe now be a little bit more concrete? What does this mean in cyber secure world? What is this threat?

00:05:02,620

Luigi Bruno

So, the threat is usually someone, so think about the malicious, so an attacker that has find out that your password is the name of your dog, and so there you have a vulnerability, which is the weakness of your password. At the same time, you have a threat and is that somebody knows what's your password. And this person might have access to your system, to whatever files you have there, right? And so, this is now we see vulnerability on one hand, we see threat. But we also see risk, right? The risk that we can calculate obviously is what's the likelihood that someone will actually breach your files because they know the name of your dog

So, we have introduced now three terms, right? Risk, threat, vulnerability. And if you sort of think about it how I phrased the attacker, I call it a malicious actor because a lot of people call them hackers. But hackers is a neutral term. I mean, hackers can be a bad person, but can be also a good person.

00:06:00,790

Alexandra Andhov

Exactly. And, you know, and over the past years, we have seen a lot of hackers who had actually very good intentions, right. But I think we will leave this for the for the for the end of the talk.

00:06:16,300

Luigi Bruno

And then, I mean, this is a bit more from a practical perspective, right? We have found out threat vulnerability, risk attacker. But then, how do you sort of shield yourself from all of this? And that's where controls come in place.

So, if we look back at your example of your dog’s name password control, a control could be perhaps changing your password every week, having a policy that tells you that you have to change your password or having multifactor authentication.

So, a control essentially is like we can say that it’s set of techniques or procedures or processes that enable one person or one organisation to completely remove or reduce vulnerabilities.

So, that's where we stand a little bit right now. I know that people are really concerned about data and data is a big thing. There are laws out there to protect data, and we all care about our data. And so, let's talk about what data why we need to protect the data in the context of cybersecurity, right? And I think there's a very simple acronym to remember, and it's CIA, doesn't have anything

to do with the American agency. It just stands for confidentiality, integrity, and availability. So, if I think about my data, I really want my data to be confidential. So, to make sure that only those who ever need to know can actually look at my data, that is, like, you know, integer in the sense that, people do not tamper with my data so that if I want to look at. For instance, let's say my birth certificate, the fact that I was born in X Y Z location stays throughout my existence. And even afterwards if somebody want to trace my roots. And then availability just stands for the fact that if I want to access my data at any given time, that the option to actually access the data at that time stays there.

And so, you know, to put this in a regulatory legal context, if we look at the, and we will talk about this later, I guess the laws and regulations, but also policies that are out there for the protection of personal and non-personal data. Everything is concerned with, you know, potentially integrity and availability. And I think this is just like, you know, where we sort of stand a little bit in terms of intro.

00:08:37,370

Alexandra Andhov

Okay, so this is, let's say, the cyber-security. So, there are these different elements from vulnerability through availability and different kinds of risk analysis.

But now probably some might ask a question. OK, but how is this relevant for a lawyer? So where does a lawyer come in when we discuss cybersecurity?

0:08:53,759

Luigi Bruno

So, a couple of days ago was speaking to a friend of mine who is a is a partner at the law firm. And this law firm was started by somebody who's now in his 70s, over 40 years of experience as a lawyer. And I was asking him, how is this guy - I'm not gonna make any names – dealing with how the professionals change? And he said to me that he's really struggling because he had to hire people to just work on all aspects of the profession that are now digital, which is essentially anything other than going to court and plead.

00:09:41,210

Alexandra Andhov

And even that can be digital, and was digital during COVID.

0:09:46,840

Luigi Bruno

Even before the pandemic, and I'm so glad to introduce the pandemic, there was a wave of digital transformation that was hitting the legal profession. But that was happening rather slowly.

00:09:51,980

Alexandra Andhov

Exactly. And everyone's saying, Yeah, this is just, you know, another new version of word document coming in and everyone is like, but we don't need this and so on yet.

00:10:02,190

Luigi Bruno

But then when the pandemic happens and it's like, boom, everything becomes digital from one day to the other. And obviously, what happens is that you've just paved the way to vulnerabilities to surface, to threat to happen. And then you also have a lot of risks coming from this.

And you have a lot of attackers potentially, you know, malicious people that if, before they needed to physically breach the premises of your law firm to get access to your client files or to eavesdrop on a conversation involving a patent for industrial espionage, now they can just eavesdrop a conversation or steal one of your emails, and they can actually, you know, breach your attorney client privilege.

And so, here is like just a little bit of a context of why cybersecurity has become really, really important for the legal profession. And I think in general the fact that the nature of the legal profession itself, it's so hinged on the preciousness of information makes cybersecurity even more relevant for lawyers. But in general, notaries, judges, the court system, everybody that's involved in the overarching justice system, and that's where I think it's really important to keep in mind that that we're not going to go back to pen and paper, we’re going to stay as it is and cybersecurity. It's as important as any other aspect of this.

00:11:32,750

Alexandra Andhov

Okay. But, because you said that you were teaching a course on cybersecurity at McGill, and I wonder how this field, which is part of the digitalisation it's coming into the education of the lawyers. Because one can say all the examples that you mentioned that someone can steal your email or eavesdrop on your conversations about patent or access different kinds of know-how documents in your M&A, that is happening, in order to offer a better bid or whatever is there.

One can say, of course, we understand the risk, but this is not lawyers’ job. This is a job of, let's say, of an IT specialist whose obligation or duty is to protect our data and how we communicate

as lawyers. So, when you were teaching the course, in other words, where did the law as a lawyer or our legal activities coming to cybersecurity?

00:12:36,269

Luigi Bruno

So, I mean, obviously, first of all, there's a big difference between big law firms that they can actually afford to have IT staff on payroll and, you know, single practitioners or freelancers that really have to do everything by themselves.

And so, I think in general education is really relevant because education doesn't differentiate by your revenues but really aims to educate everybody. And it's only by sharing knowledge that we actually achieve the aims of cyber security, and that is we have strong protection.

But that said right, I think one of the main aspects is the fact that when you pass the bar you have obligations *vis a vis* your clients and obligations *vis a vis* the justice system. And so, it's your responsibility to satisfy those obligations.

And so, like, one of the questions is, so you have to maintain attorney client privilege, right? But does that mean that if your client data is stolen from your laptop, are you breaching attorney client privilege? And so that's like something that needs to be considered because if that's the case, you know, even if the ethics rulebook of your particular jurisdiction doesn't talk about cyber security. But just let's talk about, you know, attorney-client privilege, then it's up to you to interpret how you actually, you know, take care of that.

And so just one angle. And then if we look actually at the regulation out, existing regulations. I think there's a very different context in which cybersecurity becomes relevant *vis a vis* law.

So, you have obviously the criminal acts that are perpetrated online. So, think about I don't know, improper access to computer systems, right? That's criminally liable. And you know that's relevant, of course, for criminal lawyers, but also for other.

And then you have the various, the various regulation that's concerned with the protection of data I think about, for instance, GDPR. It's obviously concerned with the protection of personal data. But how do you protect personal data? Article 32 of the GDPR it’s actually a cybersecurity article because just the title it's the security of processing activities, and then it tells you that you as an organisation, have to put in place a technical and organisational measures. And it lists some of them, like encryption, demonisation and so forth. And those are clearly, you know, cybersecurity activities. They're not necessarily legal activities.

And you also have international law, which is concerned with cybersecurity because it becomes, you know, relevant *vis a vis* warfare. So, you have the famous Tallin manual, which basically gives you a definition of what cyber warfare is and tells you how that needs to be seen, what are some of the acts that are sanctionable, not sanctionable and so forth.

And so, I think that’s a multidimensional relationship between cybersecurity and the law. And obviously the role of lawyers is everywhere in all of this, in a sense that it's not just like protecting

themselves and their clients, but it's also in the fact that how the profession is evolving, not only in just like being digitalised but also in what are the matters the lawyers are called to deal with. Because there's so many different matters the lawyers are called to represent their clients in that involved cybersecurity and the protection of data, and also IP.

00:16:11,389

Alexandra Andhov

So, I'm hearing what you're saying is ultimately that the cybersecurity knowledge, and of course we ee that there is more and more regulation coming also in this area and I think we will need to talk about it next time. But the fact that this is becoming part of the portfolio of any lawyer who is going to deal with IP or generally data protection.

00:16:36,960

Luigi Bruno

Yeah, I mean, even M&A. Part of my job is that you know, when we do due diligence before assessing a potential acquisition, we really do a thorough cybersecurity due diligence. And the reason is because I mean, if you are investing, if you're acquiring a company or even just as a venture capital fund or private equity fund and you know the cybersecurity posture of the company you're investing in is terrible and they suffer a cyber-attack or they suffer a data breach because, you know they haven't protected their data, your return on investment is going to suffer massively because at the end of the day, you know, if you lose your customers' data, your brand is going to be damaged, your bottom line is gonna be damaged.

And so, I think there's a at the end of the day cybersecurity is really central to all sorts of economic activities right now. And lawyers have such a sensible duty *vis a vis* economic activities because they need to make sure that the represent their clients' interests, but also overall, they're central to the functioning of the justice system. And therefore, it's I think, for me, If I were to go back to law school now, I would really want a programme where they teach me cybersecurity. Because at the end of the day, I want to be educated on this. I want to make sure that they can do the professional accordingly to the times.

00:17:57,630

Alexandra Andhov

Excellent. Thank you, Luigi. And I hope that everyone who is listening will do a little more of maybe research on how they can educate themselves in regard to cybersecurity for their own activities, but also to support their clients.

Again, thank you Luigi for joining us. Thank you, everyone for listening.

We will continue to bring you different legal tech topics.

This is the Copenhagen Legal Tag Lab podcast.
Thank you, Dreyers Foundation for supporting us. My name is Alexandra. And have a nice day.

00:18:34,859 - outro
This is Copenhagen Legal Tech Lab podcast at the Faculty of Law, University of Copenhagen.
Brought to you by the Dreyers Foundation.
And don't forget to subscribe and follow us on social media and your favourite podcast platform.