Knobbe IP+

PODCAST

European Union AI ACT: A Discussion with Hanane Fathi Roswall

Mauricio Uribe
Partner
Knobbe Martens

Hanane Fathi Roswall
Partner
Aera IP

HFR **[COLD OPEN] So when should companies pay close attention to the EU AI Act? I think they need to do it now, as long as they have a plan or they already have products in the EU market for sale that involve AI systems. And I think there's a lot of preparation that needs to be done. The EU AI Act is here and it's going to be starting very soon, to start to be enforced. So, "preparation" is the keyword today.**

MU Welcome to this episode of the Knobbe IP+ Podcast. I'm your host of today's episode, Mauricio Uribe, a partner at the law firm Knobbe Martens. Today I have the pleasure of speaking with Hanane Fathi Roswall, a European patent attorney and litigator and a partner at Aera IP. Welcome Hanane, how are you?

HFR I'm very good. Thank you, Mauricio. It's a pleasure to be here.

MU Well it's a pleasure to have you. I think this will be very interesting. Today we'll be discussing the EU AI Act, what you should know, why this is important for companies all over the world. Before we get started, let's tell the listeners a little about yourself if you don't mind Hanane? What's your educational experience, your technical background, and some of your legal experiences?

HFR Sure. Actually, my background is in electrical engineering and telecommunications and information security. So I was a scientist for a long time before I turned into becoming an attorney and finally founded this firm. And so I've worked in Japan and in Europe. I'm actually French, and I live now in Copenhagen. Very European, but I think its very interesting to have different viewpoints. And in the technological field in which we've evolved, there's just so many different viewpoints from different parts of the world. And so that's what I try to admit into the patent space and intellectual property. So I've been protecting AI-based inventions for probably a decade now, and that's a very interesting field that's also being discussed a lot on patent and other fronts. And that's why also we've been very excited about the EU AI Act because it has become also a societal topic that the EU Commission is trying to address, and that touches upon these

regulations and legal framework. And so that's why I'm really excited to have this discussion today.

MU Me, too. And I think a very timely topic because not only, and hopefully you would agree, that AI has seen an evolution in terms of the technology, what we're now seeing here is what may be one of the very first governmental or organizational acts towards the use of AI. So I think we're very much on the front end of this topic and so I think for our listeners, just a wonderful way to get to know. So if you don't mind, let's really get into it. What is the EU AI? What is the purpose of this sweeping set of regulations?

HFR That's a good question because at the bottom, no one likes too much regulation, but somehow we need some regulations. And I think its quite brave of the European Commission to try to address this. And nothing is perfect but I really like the exercise that they are trying to do to have certain principles. And certain principles that are sorted into risk and trying to protect our fundamental rights as citizens of the European Union, but also some aspects that are more rooted in technology and trying to define what is AI or general purpose AI. And I think that's a difficult balance to strike. And therefore the purpose for this is to have a comprehensive legislation or legislative approach so that we have a responsible use of AI systems in the European Union. And I think the more high-level purpose is to somehow provide some protection to our fundamental rights and liberties. And so I hope this helps a little bit at the high level and a little bit at the lower level, too.

MU Sure, and I think that we'll drill down specifically into the details because I think those are – for our listeners – are going to be incredibly important. But one question I had for you there: is this something that you believe will be addressed at that higher level of the European Union as the enforcement mechanism? Do you anticipate that individual countries will have some role then, as individual members of the EU? Where does this lie within that hierarchy?

HFR I think it's a very interesting question but for now what we know, because this is all new, is that we have the European Commission that has done this act, and there will be national authorities that are competent and have oversight power as member states. And what I think looks promising is there will be an EU AI Office that has a little bit of functional independence and is linked to the EU Commission. But the hope for the AI office is to provide us guidelines that we are really expecting, and guidance so that we know how to comply and whether you comply, and to what extent you comply, and in which category is your AI system falling, and what are the risks associated. So I think that's a good thing. And there are other bodies like the AI Board that is representing the member states and providing the more strategic oversight for the AI Office. And there's also some scientific independent board that supports the activities of the AI office. So the idea is to be able to cohesively progress and provide guidance for the rest of us users and lawyers…system providers, product providers, distributers, et cetera.

MU You know it's interesting—in your last answer you bring up a great point. And this is something I always enjoy talking about when we look at topics such as regulations or policies. Maybe perhaps it's less focused on the enforcement mechanism. I know that's

an important aspect, but if these are the regulations and these are the guidelines by which companies will interact, perhaps if we all conform to that and everybody complies with it, there will never be an enforcement of the EU AI Act because everybody will kind of move along the way. And maybe that's a good thing for not only for the EU but maybe the world.

HFR That's what I'm hoping. I was thinking actually today that from a European point of view, we think that GDPR has helped pave the way for other privacy regulations in the world. It's maybe a humble European euro-centric position. There may be some idea of okay, the EU AI Act may be paving the way but if you have to derive principles of law so that there is some expectation of clarity for compliance for companies, then this is the EU Commission trying to achieve that. And that's the first that I know of. It's one of the early pieces of law that deals with trying to regulate AI systems. So could it pave the way as Europeans think the GDPR did? Could the AI Act do something similar?

MU Sure. I suspect this is not going to be the first nor the last of comparisons to the impact, maybe, the EU AI Act will have similar to the GDPR by way of analogy or comparison. I think that's very accurate. Now if you don't mind, I'm based in the United States and we're going to get right to the key question: How is this going to impact companies? Is this something limited only to EU-based companies or companies with a strong presence in the EU? Or is this broader reaching to companies around the world?

HFR I think it has a reach for any company that comes into the EU market with their product – either directly or through distributors, employers, importers. So the moment any of these products may rely on some aspect of AI operation or machine learning operations, then those are the companies that are concerned by this act and should be starting to prepare for compliance if they want to proceed into the EU market, the European Union market mostly.

MU So certainly a broader sweeping impact there for us.

HFR Yes.

MU And so before we go into the details of what exactly does that mean, I want to talk about timing because I know we're early in the process. And maybe you could explain what is the current status of the EU AI Act? What are going to be the likely next milestones as it progresses towards adoption or ratification?

HFR Yes, very good question because its all about timing. And I think that's why I think its great that we have this discussion today super early. In December 2023, four months ago, the European Parliament and Council of the European Union reached this political agreement that is the EU AI Act. I liked that on LinkedIn saw "Habemus EU AI Act." You know, "Habemus papam, We found a pope." It's like, "We found the Act." [Laughs].

MU [Laughs] Yes.

HFR And I think it is because it's a collegial effort in these type of bodies. So the next milestone is that it's been formally translated and adopted, but then it has to be published in the official journal. And that's where time takes off. And then 20 days later

it starts to be applicable. It's in phases. There are some like those prohibitions for "unacceptable risk," those that are really prohibited, within six months. And then there are others that are within 12 months, like for the "general purpose AI models." And then those that we will maybe discuss the "high-risk" or "limited risk" AI, those are within 36 months that they'll have to start to be enforced. So that's what companies that have stakes in the EU, have products or decide to launch or enter the EU market with their products, have to think of. And some say, oh it may be very soon – this publication in the official journal. Maybe it's June, maybe it's September. So the start of the ticking time is quite near but the progression to full-fledged is over two and a half years or so.

MU Interesting. So that kind of brings up what I would assume is the next logical question for companies that might have applicability as you said. Now that it's a worldwide problem, when's the right time for companies to begin preparing themselves? We're going to go into details, and it does seem there are requirements or obligations for these companies, and I would think some of those would require preparations. So when's the right time for that to start thinking about it?

HFR Yes I have to be honest—I think it's about now. I think usually most of the companies know to which extent they use AI in their products that the distributors sell, whether they know the European Union market is a market of relevance. And so basically it's now time to start to have an inventory of AI systems that are being developed in your product or being deployed. And then to determine whether any of these systems are within the scope of the AI Act at all, and start to see are they in scope, in which category et cetera. Because I think it's not a small compliance task to do because we will be the first one to test it. So I think it's now. So that's why I think this conversation is very timely.

MU I was just going to say your most recent answer just give me all the more reason why I'm so happy we're having our conversation today because it does seem like we need to start talking to companies and companies need to start talking about this and then planning for it. So, fantastic. We're going to take a short break here.

A reminder listeners, I'm Mauricio Uribe with Hanane Fathi Roswall, and we're talking about the EU AI Act. Hanane, we've covered the general aspects of the EU AI Act. We've talked about the timing spread out but we need to start thinking about it now. I'd like to drill down for the remainder of our podcast today. What exactly is the EU AI Act? And maybe we'll start with the definition. The term "AI" I've always thought was just so broad. It can mean a lot of different things to different people. So what does it mean in the context of the EU AI Act?

HFR That's a good question. I think the people that have worked to craft this act have also been trying to define this in the most legal certain way, but the definition that is provided in the law is this that includes any machine learning approaches. Then it becomes technical: supervised, unsupervised, reinforcement learning – using a wide variety of methods. And it's also related to the logic and knowledge-based approach. That's also quite technical…and auto-statistical approach like Bayesian or search and optimization methods. So that's really specific technically you would say, right Mauricio, for us that

are engineers that are in this field. And so the important aspect is to understand that it's also being able to generate output and that this output is based on this input, and what's in between was what I've just explained—all these different approaches of the machine learning techniques. And that these outputs can be like these predictions, recommendations, but somehow it seems to be linked to some kind of decision or some kind of ability to control based on that output.

MU Okay. Do you suspect that the intent behind this initial definition of AI was meant to be very broad to cover quite a bit of technology or was this more intended to be a starting point with maybe a more narrow focus? And where is that trend going to go? More broad? More focused?

HFR Yeah, I think my personal opinion is I think its maybe over-broad. And then I'm wondering if it's the current situation that requires this. Because these are a little bit black box systems and whatever is "black box," it is "Oh, we really have to regulate and we have maybe to go over broad to start." So let's see how the guidelines are going to play a role there. Are they going to define the breadth? Or are they going to focus it a little more to something that we can use? But I think its also very interesting how the AI systems, the "high-risk," the "limited-risk," the "low-risk," they are defined in this very broad way.

The general purpose AI is defined in a very specific way. We're determining in terms of floating point operations and it has to be 10^{25}, and for now it's like super-super computers that can achieve that. So I think I was puzzled by the spectrum there, that these AI systems are very broadly defined in my personal opinion, while this general purpose AI is like the number of floating point operations. Let's go there. And so I'm hoping that at least these guidelines from the AI Office, they will help bridge, understand how broad this is really, or will we have a more concrete interpretation that we can work with.

MU I find your observations just incredible because I completely agree, and my worry would be overbroad but like you said, it does seem to combine the two. Do you have the sense of what's going to be that mechanism for updating this listing? I believe it's Annex 1, but it might be something different now. But what's the mechanism for updating this definition of what's covered in AI?

HFR So the way I understand it, is that the European Commission is capable and has the permission or the right to update. And so I think it's going to be therefore interesting once it's enforced and starts, and we start to see in which way this is to be interpreted and whether actually indeed the European Commission will go back and make adjustments.

MU So we've kind of talked now, and you mentioned in your answers a couple of times, the pyramid of risk right? That to me strikes a by far the most substantive question we have. We now know AI is there, we know when this act's going to be done, but what does it mean in terms of what are these regulations and how are they organized? So

maybe we'll start with if you don't mind, just an explanation of what is being referred to as the pyramid of risk and then we'll drill it down to what each of those might mean.

HFR Thank you. I think it's very interesting. I'm actually thinking that the EU Commission didn't do such a bad job in a way. That okay, they came from a risk point of view and the highest risk is to preserve our liberties and our fundamental rights and protect the vulnerable persons or citizens. And so they drew a line there and said, "Okay, this is unacceptable. The rest – let's work with the grey zone there." And I think that's why this pyramid – it's a nice principle that is risk-based. And so the highest risk is to lose – or that our fundamental rights are violated or corrupted in some way, and in a way that may not even be perceptible by us. That's like the highest level of risk. And then we draw the line after that for high-risk AI systems and minimal risk AI systems, and that's where I think its not an easy exercise.

But the one that is completely permitted and you don't need to do anything regarding that, is when it's not covered in any of the two other categories. So it's like, how do you call it, you take the lower bound, you take the higher bound, and now we can focus on those that have high risk or minimal risk where this is still some compliance to do. So that's one approach.

MU Yes. I really like the practical description you have. It's a wonderful visual, if you see it in EU documentation, of this pyramid structure. But I really like how you drew that out of saying the upper bounds of this pyramid if you're using the visual, or the high-risk and then the lower, the base of the pyramid of the low or minimal risk and say, "well the reality is we can deal with those fairly edge cases well. And maybe our focus is going to be in that middle." And I really liked how you grouped that together. I think from a practical standpoint that makes a lot of sense. So let's talk about the top of that pyramid, the "unacceptable" risk. We'll follow the same format if it's okay with you to just kind of help our listeners. What are these technologies? They're "unacceptable." We have guidelines but what are those? What are the technologies?

HFR Yes, that's a very good question. So it's these that have to do with exploiting some kind of vulnerability or manipulating a specific type of group but in a way that we are circumventing their free will to cause harm. Like, if you're manipulating a child into buying certain things that they don't even realize they're doing that, or you're monitoring them to an extent that is a violation of their rights. Or also all aspects of, we're very – I'm also French, so its even more for French. Everything that is social scoring or anything where you start to classify individuals based on certain characteristics that are not objective and is leading to detrimental treatment or leading to that possibility. So, I think one should be wary whenever the system – because the system always needs some kind of information about the user right? Like you need to know what the user, who the user is to some extent. There is some information even if you just have a user identifier, it may have other information to which extent this can be seen as social scoring. And I think that's a little tricker if you're having a system that also is able to deal with sensitive data. Like "What is your race?" That's not allowed for example in France. Or, "What is your religion?" It's also not allowed to even hold that piece of data. Or sexual orientation. And then you infer some kind of categorization.

And also nowadays, we have a lot of facial images for opening of our phone or various things, and I think that's okay because it's local, but the moment you start to have this in a higher collection like monitoring or scrapping facial images from CCTV or the internet to populate a database, to control a further process, that's I think where these are the upper bound, the unacceptable risk.

MU And then one question and maybe there is no clear answer. If I'm a company, how do I know I'm in this unacceptable risk? Is there an authority that will tell me, "Yes, this is unacceptable risk?" Is it self-reporting, self-analysis? I'm assuming there's clear connect cases that you described with some of them? There might be some edge cases where I'm providing a supporting component or some manipulation of that? Do we know right now what that will be, what that mechanism is?

HFR We do not know right now but to be on the side of precaution, I think its good to whenever, for example, you interact with specific groups of individuals like children or disabled people with disabilities, or you're starting to infer such characteristics based on certain characteristics of a person and for certain behavior, or try to classify in this way, I think we start to enter the zone of whether it's prohibition. And I think that's where one should seek counsel and to be able to identify that. As such, we don't have an authority that will tell us yes/no. Also for the other, the in between, not the high, not the low, there's like self-assessment. There's also – you can use a third-party to help you, but it's all the homework of the companies to do. And therefore to seek also external help if they don't have it in-house.

MU Okay. So let's turn then to the high-risk category. That level in the pyramid, from my observations, seems to have the most type of responsibilities or obligations. What are some of the technologies or what are the guidelines for a company to know I may have something that would be a regulated high-risk AI system?

HFR Well I think for example you can think anything that has to do with biometric identification and surveillance, like in recruitment software or medical devices or automotive. But also you could have systems that are enabling access to essential services like the banks or insurance or credit worthiness, benefits. But also there's this really—I think it's more what's important for a country, like critical infrastructures like hospitals, electricity, certain things like that or energy transport that are in this category. So I hope this helps a little bit for the listeners to understand to some extent what is high-risk AI systems. It's in these spaces, as examples.

MU And if a company has a product or thinks they might have a product in this space, what would be the requirements for that company to do? If it falls within, if it isn't banned, so where are they at?

HFR I think its quite a long list of requirements, but it also depends. If you're a provider, you have a certain list. And then you have, if you're an employer, an importer or a distributor, but nevertheless, all of these have—at least you have to have some kind of transparency and inform the user that this is an AI-based, or high-risk AI-based system. There's also the ability to conduct human oversight that is in all of these and have a certain level of security. So all of this needs to be established and documented to some

extent that you have good data governance over this. And there will be a new – the plan is to have a new database where you can register these systems before placing them on the market. And so that's for if you're a provider of that system. And you can also go to a third-party that can help you get the assessment from an accredited body.

MU And so maybe the close of that, if you're a company, where's the responsibility for this? Is this something I can outsource completely? Is this a combination of third-party vendors, attorneys? Do I need in-house resources that can commit to doing this given that you said it's a fairly extensive requirement?

HFR That's true. I think it depends on the scenario but in any case, you need the homework in-house to be able to know, "Where are the logs? How are we informing the user?" Are these technical solutions that need to be in place around these AI systems? So that's usually—the company should provide this information. And then to know, okay, is this sufficient information? Is it sufficient log? Is it transparency? Data governance experts would be needed in this. And then you can also decide to outsource a part of it, but I think it's a collaboration between the in-house people, the company, and the experts in EU data law.

MU So let's close out then –limited risk right, that third level of that pyramid. Again what would be some of the—how do I distinguish between high risk versus limited? What are the technologies and what are the limited risks?

HFR Yes that's a good question. Let's see for this. Those that still need some requirements is like the systems that directly interact with people like a chatbot or certain things like this. It's important for the user to know, oh I'm dealing with – this is not Mauricio. This is a chatbot, having a nice appearance of Mauricio. [Laughs] There is this level of transparency for these types of systems. Like if you're manipulating for deep fakes, I know it's a big deal nowadays, but those are also under that limited risk.

MU And then what would be the requirement for that? I know transparency is the keyword.

HFR Yes—

MU Is that a different level of conformity than the high-risk for that or is it similar aspects of that?

HFR I think it's similar aspects. I see it as, they all have this basic box of compliance. That's like transparency, informing the user, those are like the basic boxes. And then the high-risk, there's more boxes on top which we just talked about. But there's definitely this need to obtain the consent of the people exposed to this. There's also some AI solutions that are falling under that category that have to do with emotion recognition or certain things like that.

MU And I think given the second part of our conversation today, not only will this EU AI Act have a wide sweeping applicability to companies around the world, the requirements are fairly extensive. Is that a fair conclusion to walk away? It will require a very detailed plan and thoughtful execution by companies, and it seems to apply to a lot of different companies.

HFR Definitely. I completely agree. So that's why I think, when you asked the question earlier, "When should one start preparing?" I'm thinking about now to figure out what all of these aspects because they are a measure of legal and technical aspects. So you need to have the interaction between these two teams to be able to fulfill the evidence and all the safeguards that they are requiring.

MU Well Hanane, I think we're out of time for today, but this is –I suspect, this will not be our only conversation on the EU AI Act. There will be lots of subject matter to discuss, but in terms of raising awareness, thank you for that time. That wraps up today's episode. A big thanks to our guest Hanane Fathi Roswall for joining us today. Be sure to visit Knobbe.com to listen or view the written transcript of this conversation or other episodes of Knobbe IP+. Until next time, thank you very much.

59150659