ICANN74 | Policy Forum – At-Large EURALO Policy Session: Laws and regulations in the European Union
Tuesday, June 14, 2022 – 13:15 to 14:30 AMS

YESIM SAGLAM: Hello and welcome to At-Large EURALO policy session Shape the EU's Digital Future: Sovereignty, Legal, and Regulatory Frameworks. My name is Yesim Saglam, and I am the remote participation manager for this session.

Please note that this session is being recorded and is governed by the ICANN expected standards of behavior. During this session, questions or comments submitted in chat will be read aloud if put in the proper form as noted in the chat.

Taking part via audio, if you are remote, please wait until you are called upon and unmute your Zoom microphone. For those of you in the main room, please raise your hand in Zoom and, when called upon, unmute your table microphone. In the secondary room, please raise your hand in Zoom and go to the standalone mic when called upon.

For the benefit of other participants, please state your name for the record and speak at a reasonable pace. Onsite participants may pick up a receiver and use their own headphones to listen to interpretation. Virtual participants may access the interpretation via the Zoom toolbar.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

With that, I will hand the floor over to Pari Esfandiari.

PARI ESFANDIARI: Thank you very much. Welcome, everyone, and thank you for joining us today wherever you are. It's a lovely European day here in The Hague and it is so nice to see some real faces again.

This is the At-Large EURALO policy session titled Shape the EU's Digital Future: Sovereignty, Legal, and Regulatory Frameworks. My name is Pari Esfandiari, and I represent ALAC EURALO. A very popular and familiar face within the ICANN community, Olivier Crépin-Leblond, will join me via Zoom. Together we have the pleasure to moderate this session on behalf of the At-Large community which strives to safeguard the interests of end users.

This session has a strong end user component, the digital security. The European Commission has recently initiated a number of projects and regulatory proposals to ensure security. This session aims to understand the impact on the Internet community. Next slide, please.

I would like to explain how we plan to conduct our discussion. The session is composed of five parts. First, I will introduce the topic, explain the motivation for this strategy, and introduce the proposal initiatives to set the context.

Next, Elena Plexida from ICANN Org will explain ICANN's position in relation to these potentially challenging regulations and projects.

After that, we will have three accomplished representatives from three Internet communities: Polina Malaja from the Council of European National Top-Level Domain Registries, Lucien Castex from AFNIC, and Chris Buckridge from RIPE NCC. The representatives will share their reflections on how these developments impact their respective communities.

Next, we will welcome questions. Already, you were provided with the instructions on how to post a question.

And after Q&A session, finally in the last part, we will have Olivier who will share the closing remarks. Next slide, please.

Now first, in order to understand what is happening and project to the future, we need to look back and see what are the motivations and concerns that these initiatives are coming about. So EU has been concerned with the level of national infrastructure resilience, dependence, and vulnerability.

This concern is motivated by a number of issues. Increasing reliance of critical services on digital technology. Central role of digital technology in geopolitics. Decline in European digital enterprises. Dependency for services on foreign-owned and controlled enterprises. And increased geopolitical tensions and cyber-hostility. Next slide, please.

It's within this context that the European Commission on December 2020 announced a series of initiatives which outline major EU policy objectives in the field of cybersecurity and technological sovereignty. These include the Communication on the EU's Cybersecurity Strategy for the Digital Decade, Revision of the Directive on the Security of Network and Information Systems (NIS2), and Directive on the Resilience of Critical Entities including an initiative for DNS4EU. Next slide, please.

NIS2 is a revision of earlier directive on network and information systems. On one hand, it aims to increase member states' preparedness and cooperation. It establishes the European Crises Liaison Organization Network and also discusses the access to information. This is about data sharing between nations states. On the other hand, it aims to promote a culture of security across critical sector enterprises.

So who is targeted? Operators of essential services. Digital service providers including online search engines, online marketplaces, and cloud computing services. The regulations do not apply to small digital service providers.

And what are the requirements? Risk management measures, reporting obligations, and prevention measures. The Article 23 of the revision is particularly criticized for compliance challenges and also for bypassing the multistakeholder model. Next slide, please.

The DNS4EU is another initiative to exert control over the DNS. it aims to address the vulnerabilities caused by consolidation of DNS resolution. And there are debates whether it really resolves that consolidation and creates diversity or actually creates more consolidation. It also provides partial funding to construct DNS resolver services in the EU which raises concern about data sharing obligations. It's not clear on that at this point.

As you can see from this brief introduction and you will hear from our panelists, the Internet community wholeheartedly supports the motivation and objectives that form the foundation of these policies. But as usual, the devil is in the details.

We now turn to our speakers who represent different parts of the Internet community to learn how their communities perceive this legislation. Next slide, please.

We will start at home with Elena Plexida from ICANN Org. She will discuss the ICANN's perspective on this legislation. Elena, the floor is yours.

ELENA PLEXIDA: Thank you so much, Pari. Hello, everyone. Let me start by saying I feel very, very strange in a good way to be doing that not on Zoom. So I have forgotten how to do that, so bear with me. Thank you. All right, today we have been asked to discuss basically about the DNS4EU and the NIS2 directive.

I don't need to make more introductions. Pari made them already perfectly well. I put the slide just to show you that those two initiatives—the one is a legislative initiative, the other one is a non-legislative initiative—are part of the same package. It was a package that came out in December 2020.

It included a strategy. This is the non-legislative initiative. The strategy is a set of actions that the European Commission is putting on itself to carry out itself. It was in there that we had the DNS4EU. In there also related to the DNS I just wanted to mention there is an idea that there needs to be a contingency plan for the root. This initiative is still just the [inaudible] in the strategy with no more details. And we are looking forward to see more of what the commission is thinking there, and particularly what is the problem definition.

And the other part of the package was, as Pari mentioned, NIS2 directive and another directive as well on the resilience of critical entities which I have not included in our slides because we didn't see from our perspective that [inaudible] on the DNS.

Okay, going to the DNS4EU, which is an idea, a project for an EU based recursive DNS resolver, at the strategy level when it was published there were few details available. But then later on there was a call [inaudible] that was published and provided more details. That was open until April 2022.

Unless I am terribly mistaken, the selection process is still ongoing. Yes, thank you for confirming. We don't have someone announced that is selected to carry out the project yet. From ICANN Org perspective we don't really have a view nor a position on public resolvers provided either by companies or by governments. There have been other DNS resolver projects around the world with government support or involvement, for example, in Canada. As long as there is no mandatory use of a resolver by a government because there you open up a different discussion, the principle is the more resolvers we have the better.

What we did look into however was really the premise on which the DNS4EU was launched. And to be more particular, the market consolidation. So as Pari mentioned before, one of the key concerns based on which the DNS4EU initiative was launched was that there is a market consolidation [inaudible] significantly relies on a few public resolvers. Namely in this case Cloudflare and Google, which are non-EU resolvers.

Okay, so that was the key problem definition. And as I said, we looked into it. And I would like to pass the floor quickly to my colleague Alain from OCTO. Our OCTO team did look into the market consolidation, and Alain will show you our findings. Thank you.

ALAIN DURAND: Thank you, Elena. I hope you can all hear me because I don't have the pleasure to be onsite. Please send me acknowledgement if you can hear me.

ELENA PLEXIDA: Yes, we can.

ALAIN DURAND: Thank you very much. So as Elena said, we tried to look at the picture of public resolvers within the EU. To start with, we made a list of open public resolvers that exist, and we have a list of 29 public resolvers. So it's not just that there is a choice between one or two or three but at least 29 to choose from and maybe more. So those are the ones that we listed there.

And then we went to doing some measurements on essentially what's the market share of [inaudible]. When you do a measurement of open resolvers, it's not an easy project because open public resolver operators do not share data. So you need to make external measurements. And you cannot do that with just a few samples, even a few thousand samples place in different locations, because it might be biased. You need to have a very large campaign.

So we did some partnership with APNIC and APNIC Labs [inaudible] to use a system that sent millions of measurements per day. And we did that throughout an entire month. In January of this year we compared with also last year, and we got some results. Next slide, please. Thank you.

So first off when we talk about DNS [usage resolver] we're really talking about consumer ISPs. So when we looked at all the data, we tried to separate what was B-to-B, meaning business ISPs, versus consumer ISPs. Because our focus was really on consumer ISPs.

And then we also made a separation between the smaller ISPs, the medium-sized ISPs, and the very large ISPs. So small was characterized as some ISPs where we have about 1,000 probes or less per day. Medium was between 1,000 and 10,000, and large was above 10,000. And the maximum we have to give you an idea was about 70,000 probes per day.

So when we looked at those large consumer ISPs we first categorized all the results into public resolvers, and we see that only 4% of all the users are actually relying on a public resolver to do their DNS resolution. That means that 96% of them are actually relying on something else. So what is the something else? Well, 95.3% is actually people relying on the resolver provided by their ISP. And there is about 0.1% that is provided by another ISP somewhere in the EU, and about half a percent somewhere else.

But essentially, this is 95.3% of users of large consumer ISPs that are relying on the ISP provided DNS resolver.

So this 4% that are relying on public resolvers can be broken down into which resolver is actually being used. So of this 4%, it's about 3% that is using Google DNS, a little bit over half a percent that is using Cloudflare, and a little bit less than half a percent that is using OpenDNS. And everything else is statistically in the noise where we see only a few measurements here and there. So out of the 29 public resolvers that are listed before, it's not that we are lacking open resolvers. We have quite a lot actually. But only three of them have some statistically significant measurements in usage of DNS resolution.

So it's hard to say from this number that there is actual consolidation happening in the resolver market for consumers within the EU. With those numbers in mind, back to you, Elena.

ELENA PLEXIDA: Thank you so much, Alain. So as Alain showed you, there research that OCTO conducted showed that basically 95% of European end users are behind their ISPs in the country. It's a very interesting finding, so we thought we should share it with you.

Let me turn to NIS2 then. So NIS2, as I'm sure you are all aware, we have a political agreement but we have no text. This is sort of a new trend in Brussels, if I may say so. Yeah, we have a political agreement but we don't have the text yet. So we have ongoing technical meetings.

Now from ICANN Org perspective there were really two sides of the NIS2 that we were looking into. One of it is the scope of application on the DNS and the other one is, as Pari mentioned, Article 23 on registration data.

On the first one, the scope of application, as originally proposed the scope of application over DNS was overly broad. And I mean [capital] overly broad. It was everything DNS related under scope. And of particular concern of course to us was the fact that the European Commission had proposed that the root servers are [into] scope.

First of all, the effect of having [under] regulation the root service which is offered by operators on a voluntary basis would have significant effects going forward for the provision of the service. And we were concerned that it might actually lead to less resilience for the root server system. Because you know, the resilience of the DNS relies on the numbers. If operators or instances felt like they should [retreat] from the service, you would end up having less resilience.

And also the other big concern, of course, was the actual support to the multistakeholder governance, to the multistakeholder approach of managing the Internet unique identifiers. Which was a concern particularly coming out of Europe. They are not included in the final, what seems to be the final text. No one has seen the final text yet. And I have to say the bulk of our engagement really was on that, on the scope. We have again [inaudible] together with our RIPE colleagues, our [inaudible] colleagues.

Now still the scope is on the DNS overall rather broad, if I can say so. They cover both the authoritative side and the recursive side. At least they tried to limit it a little bit, but still I have to say that it will apply to more or less any DNS service resolver. And what I have to highlight here, it will also apply to country code operators not only within Europe that were already in scope in NIS1 but also country code operators of other countries. And CCs are a national resources [inaudible] that is a question.

As regards the registration data provisions, Article 23, they are making a collection, maintenance, access to registration data a legal obligation. In that sense when we get to implementation there could be some merit for the issues that the ICANN community is working on. And I'm saying that in the sense that when you have a legal obligation put down in a law to collect, to maintain, to give access, then you have a different legal basis under GDPR to process this data.

The processing right now it taking place under 6.1(f) which is the famous balancing test which is a question mark. Have I done the balancing correctly? Am I going to be fined afterwards by a data protection authority because maybe I made a mistake? Whereas now having it in a law it gives you the 6.1(c) legal basis to process which is I do it because I have an obligation under law.

That might sound positive. Let me get now to the other side of it. The other side of it is that Article 23 is actually intruding into the multistakeholder policymaking. And also on top of that, it does not recognize the independence of the ccTLDs. Of course, in the context of the multistakeholder policymaking, ccTLDs are independent. And again, I'm not only talking about European ccTLDs but other ccTLDs too. Anyone who is doing business with Europe is [under scope].

Now why am I saying it's intruding into policymaking? So the way Article 23 is drafted and because it is a directive, so to implemented it has to go back home to the 27 countries and they have to do national legislation. They will most likely put in place 27 different registration data policies including for which data to be collected.

So we might end up with a situation where we have the global policies made here plus the 27 ones from each member state. And these 27 ones, if we get to this situation, are not going to apply for their country codes only. They will apply for the country code and anyone who is doing business with the [said country]. That's fragmentation which is not good for anyone, not only the industry but also the end users.

And again, as I said it is an intrusion to the policymaking. We're here to make global policies that are applied globally, so it would have this thing working. It's not really a good outcome. Of course, we have implementation going forward. Once the NIS2 is adopted there is implementation we see.

So overall—and I will finish with that—we see the concept of digital sovereignty playing out on the DNS. If I'm able to [inaudible] DNS. I have to speak slower. So as I was saying, initiatives targeting specifically the DNS. EU regulation taking over bits and pieces of the policymaking. Thinking of regulating the roots, as I explained before, which would be one jurisdiction imposing unilaterally a legislation over the root.

Now of course, every government and every regional organization has a duty to protect the citizens. That is perfectly understandable. It is not only the EU that is thinking this way. And when it comes to the DNS though to the unique identifiers overall, the way to protect citizens is to make sure the global Internet works. That is what the multistakeholder governance is there for, the very reason it exists. Making policies that apply globally to the identifiers, therefore ensuring we have one set of identifiers and that is one Internet at the end. Thank you.

PARI ESFANDIARI: Thank you very much, Elena. That was both interesting and enlightening. I now would like to turn to our next panelist Polina

Malaja, policy director at CENTR. Polina will share CENTR's view. And I appreciate if you keep it at ten minutes. Thank you.

POLINA MALAJA: Thank you, Pari. Very happy to be here. Good afternoon, everyone. I've prepared also a bit of slides. Some of the stuff I will say today will be a little bit of recap of what Elena has said and Pari in the introduction. So hopefully, we can get through the slides quicker and get to the discussion part.

I will first start with the DNS4EU. And just to very quickly recap on some of the main points of this project that EU is attempting to fund is, as Elena said, DNS4EU is not a legislative initiative but it's a project that is funded by the European Commission. And it attempts to create a European DNS resolver service infrastructure.

Some of the main criteria. It's a [call for tender]. So all of the operators that fulfill the criteria can apply for the funding available from the EU to develop some infrastructure. And some of the criteria that is important to note I thought would be also interesting for today's audience is of course, first of all, the DNS4EU is supposed to serve the end users in the EU. So that's one of the first of the criteria.

And it of course also needs to offer a highest level of reliability and protection against cybersecurity threats. So these are primarily the technical threats like phishing and other cybersecurity threats that are threatening end users.

And at the same time of course DNS4EU also needs to comply with the GDPR and respect data protection. So in this specific area one of the criteria for the project is that the personal data of end users, of the customers, of the clients that would be using this DNS resolver service and their personal identifiable information cannot be commercially used or be monetized. So that's also an important criteria there.

And very interestingly in addition to the filtering requirements for the cybersecurity threats, DNS4EU infrastructure also needs to comply with lawful filtering obligations. That means basically to comply with national court orders and block access to particular illegal content. Next slide, please.

As Elena already mentioned, DNS4EU is primarily aimed at diversifying the landscape of existing DNS resolution services and to specifically address the problem of consolidation of DNS resolution that is, according to the European Commission, at the moment in the hands of a few companies.

And at the same time since the data protection requirements are very important within the standard, then this infrastructure also needs to conform to the latest security and privacy enhancing standards. So this means that it needs to be able to support, for example, DoT and DoH standards.

And if we're looking at this criteria, of course as it's not a legislative project, it's important to keep in mind that this criteria do not come with any harm as the cybersecurity filtering capabilities are important for any DNS service.

But also the fact, for example, on the filtering requirements according to the European Commission all the existing DNS resolution services already in place or being used by the European end users already have to comply with the European legislation. So in this sense there is no novelty in what the DNS4EU attempts to address.

And of course at the moment, there is no indication that DNS4EU can somehow be mandated by the European regulators or become somehow the most important DNS resolution service infrastructure. Next slide, please.

So just to look at some of the potential repercussions on the global DNS, of course, the fact that the EU funds a project, again even if it addresses DNS or is somehow addressing the DNS infrastructure, this per se is not a problem. Also, according to our understanding and as Elena said similarly as for ICANN, at CENTR we also do not have a position on DNS4EU considering it's a funding opportunity and it's open for everyone.

But of course for us what is important for our members and also considering that some of our members, the European ccTLDs, also already provide a local DNS recursive resolver service that is available for their local Internet communities, for us it's of course just important to make sure that such a project, such a service is not made mandatory in the EU and that other available providers can continue providing the service to the local Internet communities and there is no, let's say, giving a prioritization to a DNS4EU just because it is funded with EU funds.

And of course, it's also very important to make sure that consolidation of resolver markets is not addressed by more consolidation, specifically coming from European region.

So in this sense although there is already some of the criteria for the DNS4EU that needs to comply with European regulation, that should also be an ask for the regulators further as we move along and we'll see who will be developing the project. But it does not only comply with GDPR and cybersecurity legislation but it also is in line with the overall competition rules and that many local services continue being able to be used on national and also the regional level.

So that's just in a nutshell from our side to make sure that the diversity on the market is preserved. And it's good to have another service available for the users, but it should not be made mandatory. We can move to the next slide, please.

Now I will move on to the NIS2 directive. And specifically we'll focus on the data accuracy obligation in Article 23 that Elena also touched upon already in quite some detail.

So for us as CENTR as an association of European ccTLDs, we are of course very closely following the so-called data accuracy obligation that NIS2 will put in place. And in a nutshell, it is an obligation that will oblige all TLDs operating in the European Union. So as Elena already said, it does not mean the TLDs that are established in the European Union but all TLDs that operate that include their service are targeted at Europe. They will be in scope of the data accuracy obligation.

And what it means is that TLDs and entities providing registration services, so registrars primarily, will be obliged to keep their registration databases accurate, complete, and in some instances also verified.

The question of course, as Elena already said, the final text is not available at the moment and is still being ironed out in the technical meetings. So it is still unclear which datasets need to be collected under Article 23. And very importantly, Article 23 also will provide an obligation to respond to access requests by so-called legitimate access seekers. Next slide, please.

Yes, so what is also important to note about Article 23 is that it will also oblige to make nonpersonal registration data public. And as already mentioned, the verification obligation will most likely be in looking at the texts that were available from the negotiators. And there will be most likely a 72-hour deadline to respond to legitimate access seekers requests.

And again I have to repeat myself as we also need to really note that NIS2 is a directive. So even though when we will have the final text of the directive available, many details with regards to data accuracy obligation will be still ironed out at national level. So each member state would need to make sure, first of all, to address data accuracy obligation but to also give guidance to the TLDs and entities providing registration services on how to do this. Next slide, please.

And very importantly to also note with regards to this NIS2 directive and data accuracy obligation is that although the accuracy specifically is mentioned as essentially for cybersecurity and tackling illegal activities, it still does not cancel out the GDPR requirements. And the compliance with minimum and basic data protection principles are still in place and will be applicable to TLDs and registrars.

So these principles need to be respected, so we have to still speak about data minimization and purpose limitation under GDPR. Also, the fact that the data accuracy will address TLDs and registrars most likely. Also, we have to ask the question, who will be basically responsible for that, and the text does not provide guidance more than it looks like it might be a joint responsibility.

But again, since it's a directive it will most likely be left on the national level to decide. And finally, just to conclude on European ccTLDs' experiences, since in Europe we really have data protection in place for quite some time and before GDPR, so European ccTLDs really already have decades of experience in balancing WHOIS access and access requests with data protection.

So we really feel that data accuracy is, of course, important but at the same time the diversity of our community is also a strength of our community. And we feel that there is no need for increased harmonization when it comes to specifically data accuracy practices. Also because all ccTLDs are different despite them of course complying with similar legislation, there are still differences in eligibility criteria for domain names.

Also in availability of different tools and means to ensure accuracy on a national level. Just to see, for example, that in the [inaudible] we do not have a completely harmonized and one means or a European [right] functioning electronic identification scheme.

So in order to really inform the debate further as we go into the implementation phase and to really showcase the experience from our community, CENTR is currently working on the white paper on data accuracy practices across ccTLDs. We will be, of course, very happy to share it once it's ready.

And with that, I think this is all from side. And I'm looking forward to the discussion.

PARI ESFANDIARI: Thank you very much, Polina. That was most insightful. I now would like to turn the floor to Lucien Castex, representative for public affairs AFNIC. Lucien, the floor is yours.

LUCIEN CASTEX: Thank you, Pari, for giving me the floor. This is quite a timely debate, indeed. I would like for us to thank the session organizers and also the translator. Multilingualism and language diversity are key enablers and drivers for an open and inclusive information society. I'll now switch to French to present a few key points with French positions and also the French presidency of the EU Council. Next slide, please.

[speaking French with no interpretation]

Next slide, please.

[speaking French with no interpretation]

PARI ESFANDIARI: Thank you very much, Lucien. That was very interesting and shows the complexity of the issues that we are here dealing with. At this point, I do like to turn the floor to Chris Buckridge, advisory to the RIPE NCC. Chris, the floor is yours.

CHRIS BUCKRIDGE: Thanks. That's fine. Thank you very much, Pari. And thank you. It's a real pleasure to be here in person speaking through a mask into a microphone. It's also nice in some ways to be coming last after such good and informative speakers. And I think they've covered an awful lot which I will endeavor not to repeat but also try to keep it short because I know it would be great to hear from others in the room and online.

I'm coming from a slightly different perspective. So RIPE NCC is the Regional Internet Registry in Europe and the Middle East and Parts of Central Asia. And so we've also been very affected of late by EU regulatory developments. And I think Lucien's presentation really highlighted some of the shifts that we've seen in urgency, speed, intensity of regulatory efforts by the EU and by EU member states. And I think that was something that was already underway, but I do think COVID and the way that it's increased our reliance on the Internet and then some of the geopolitical events that we've seen in recent months have also really supercharged that imperative by policymakers to actually get involved and do something and be seen to be working for their citizens and users in getting involved here.

So for the numbers registry, and this is bringing in a somewhat different point than others have raised before, our major engagement and involvement with the EU of late has been about sanctions and the fact that EU sanctions on Russian entities have actually impacted our ability as the Regional Internet Registry to provide that registry service to everyone in our service region.

Now that's not something that is brand new. We were already dealing with that in relation to countries like Syria and Iran. But it is a real challenge to the multistakeholder global model of governance because it undermines the ability of the actors and the organizations within that model to fulfill that role.

And so the work that we've been doing primarily, well, a lot of the work we've been doing has been on compliance with those sanctions which is absolutely necessary because sanctions are serious stuff. You don't want to find yourself on the wrong side of that.

But at the same time trying to move the needle in a way that makes governments, particularly those governments who profess or who advocate for a global Internet, to actually reflect that in the way that they make regulations. And particularly regulations like sanctions which are not designed to break the Internet but have very far reaching and often unpredictable side effects, this being one of them.

So it's an evolving situation, and we have had some positive developments recently. We had first the U.S. with their OFAC sanctions put in place a general license for Internet services. The U.K. followed suit a couple of weeks ago with their sanctions regime. And most recently the EU has included an exemption in their Russian sanctions regulation.

So this is all moving toward what we hope can be a more generic and general approach that exempts core Internet functions and those who provide them from these sanctions regimes.

Additionally, I think if we're looking at the registry, that function of the RIPE NCC, we watch what's going on in ICANN in relation to WHOIS and it's not quite the same as what's happening in RIPE. The RIPE database has fallen under a slightly different category in relation to those rules. But we are having a lot of discussions in the community about things like inclusion of private data, historical data, etc.

And that's been something that's carried on in the last few years during COVID, during our remote meetings. We had a taskforce looking at the RIPE database and what its requirements are going forward. And we've had coming out of that a number of recommendations for policy or process changes which are now being discussed by RIPE working groups. So there's more information about that. Feel free to ask me, or just Google "RIPE database requirements taskforce."

Moving a bit away from the registry function that we do, and again this is starting to repeat a little bit of what Elena was saying because as the operator of K-root that's been another really significant campaign/dialogue/discussion with the European

Commission but also other EU institutions about the effort in the initial draft of NIS2 to actually bring the root server operators into scope of that regulation and the real dangers that that would pose in politicizing that root server operator role and the root server system itself.

And that's prompted us, I guess, as RIPE NCC and I think probably others in the space as well to move a little bit out of what had been a comfort zone of we're going to talk with the European Commission when there's an EU situation. That's our way in. In this case, we had to step up the game and actually start talking to European parliamentarians. So moving to a different phase of the policymaking process.

And I think that's been a good thing. It's been a positive development, and I believe I'm 99% certain that the final draft of the NIS2 directive will have removed the root server operators from scope. And that's a very positive outcome. But it does highlight that this is becoming a much more complicated and resource intensive process to actually engage on these issues at the EU level.

And I think that's just the final point there that I would make. And again, I'm coming at this from a RIPE NCC and RIPE community perspective. You could replace the word RIPE here with ICANN, and I think that's also equally valid. The fact that we have so many of these legislative proposals coming through, the fact that there is so much activity going on really means that these kinds of venues—ICANN meetings, RIPE meetings, mailing lists—are invaluable for raising awareness, helping people to understand the implications of some of these proposals, and also just planning a little bit how to respond.

Because the commission and others in the EU space have actually upped their capacity for consultation. They've started doing more public consultations. They've been more open about this, which is great. But there are so many of them, and it's hard to keep track of what's open, when, and for how long. So there does really need to be some community planning and coordination to be effective at this. And I think it's more important than ever that we do be effective. Thank you.

PARI ESFANDIARI: Thank you very much, Chris. We're a bit behind the time, so I will be quick. We have a raised hand, so I would like it to be brief. If you could please give the floor to the raised hand to pose their question.

UNIDENTIFIED MALE: Hi. [inaudible] for the record. Thank you for the presentations. First of all, I have to say I am very glad to say that for the first time since several decades it's possible to bring together the technical community in Europe and the privacy nongovernmental organizations. Usually, both of these groups have different interests, but this changed with the [inaudible] sanctions which are extended now to Russia. Because they simply say do something to the technical community, to the DNS community.

Stop spreading fake news by Russian government institutions and [inaudible] how to do this. Have you ever heard about the process which is started by [these sanctions]? It's very simple. It goes down the way to the governments. It goes down the way to the companies. Then we have large [companies with CEOs] which have no understanding of what they are talking about. That's why they are [CEOs].

PARI ESFANDIARI: [inaudible]

UNIDENTIFIED MALE: Stop, stop, stop. Just a moment, please. And finally, somebody in the [chain] decides which domain names need to be blocked. We have the same problem with the DNS4EU initiative. There is this [blocking scheme] in it. You are able to block access to domains. Why? Where is the reasoning? Nothing is there. We have an open censorship [plot hole] in this proposal, and I do not accept this.

Second point, we talked about WHOIS. We talked about the NIS2 initiative. The whole purpose of WHOIS was to get in touch with people who are running a technical system, autonomous system, a website or something like this and [someone] is not operating anymore and we need a different way to get in touch to solve the technical problem. That's three decades ago, four decades ago.

The system has evolved. Now most of the information is not accessible anymore. So the original purpose for collecting this data is not valid anymore. And if I see in the slides here that the purpose is to have accurate data in order to get access for lawful law agency or intellectual property, I'm sorry. That's not the purpose. And according to the GDPR the [preface], the whole intent of the GDPR is not to collect data which has no purpose for. So please stop this. If you stop access to the WHOIS private data which is necessary to contact somebody, then stop collecting data.

PARI ESFANDIARI: Thank you very much.

UNIDENTIFIED MALE: Thank you.

PARI ESFANDIARI: Yeah, thank you very much. Now I like to turn the floor to Olivier to pose the first question. Olivier, the floor is yours.

OLIVIER CRÉPIN-LEBLOND: Yeah, thank you very much, Pari. So many questions, so little time to ask them. Just looking at the different things, first I wanted to thank our participants, our three participants for providing us with details of those both the DNS4EU and also the NIS2 directive.

A question I had for Elena—and by the way this is just to get other people to also stand up in the queue and ask questions—the question was with regards to this whole thing of contingency plan for the root and the whole idea of making the DNS more reliable. How does that work? There are already 1,610 root server occurrences in the world, 288 of which are in Europe. How can you make things even more resilient? And are we mixing OpenDNS servers, so you know the public resolvers, with the ISP resolvers? And "we" as in not us but is Europe mixing those?

ELENA PLEXIDA: Thank you, Olivier. I missed some part of the question at some point, but I think that I've grasped it overall. You were asking about this idea of a contingency plan for the root and how it can be more secure?

OLIVIER CRÉPIN-LEBLOND: Correct. Yeah, the contingency plan for the root. And at the same time you mentioned the public resolvers, the largest of which being 8.8.8.8 and European Commission saying most of these public resolvers are foreign. And then of course we spoke of the fact or we saw with Alain Durand that the majority of resolutions took place at the ISP level anyway which is a local thing. Are we kind of mixing these issues, or is Europe mixing these issues?

ELENA PLEXIDA: Thank you. Thank you again for repeating. So to your question about the idea that there needs to be a contingency plan for the root. And as you said, there are so many [machines] around the globe propagating the same root file. And those are actually the contingency, right? If one goes down, then you have another, then you have another, then you have another, then you have another. So my answer to your question is that I'm really looking forward to the answer that we will get from the European authorities as to their thinking behind that. There is no meat there yet, and we are really looking forward to understand what is the problem here we're identifying.

For the other part with the DNS public resolvers. So again, it is one of the basic premises we heard from the commission for the DNS4EU. That there is consolidation and the bulk of the market is Google and Cloudflare. But it seems that is not the case. And perhaps, yes, I mean, as Polina was saying before, there are also ccTLDs operating these resolution services. There are many, many, many, many resolvers out there available to Europeans, and it seems that end users in Europe, actually 96% of them, are served by their country's ISPs or other providers.

OLIVIER CRÉPIN-LEBLOND: Thank you. A question for Polina because I'm seeing the time fly. You mentioned that the service could be mandatory, the use of DNS4EU could be mandatory. How would that work out? Could this bring blocking of other DNS resolvers? And in that case, are we still talking about an Internet really an intranet?

POLINA MALAJA: Thank you, Olivier, for a slightly controversial question. So of course there's no indication yet that DNS4EU might ever become mandatory since it still needs to be developed. And of course, any movement toward actually mandating any technical or technological solution within the region on the national level is against the idea that legislation in general should always be technologically neutral and also future proof.

So it will be definitely going against actually some of the basic principles that EU has also tries to adhere to at least when legislating and proposing new policy or legislative initiatives. So I think we really have to keep an eye on these developments and sometimes maybe remind also policymakers if they might forget about some of the basic principles. But yeah, technological neutrality is one of those that are key and also just a part of policymaking. But of course, we'll see as we go forward.

OLIVIER CRÉPIN-LEBLOND: Thank you, Polina.

PARI ESFANDIARI: I wanted to pose a question to Chris. Chris, what do you see as the most significant risk going forward?

CHRIS BUCKRIDGE: I think the big risk is just not being able to effectively engage because I think that's where the risk factors in a lot of this emerge. It's not to say that governments don't have a role here or that regulation is not reasonable response in some instances. It's that actually developing the kind of regulation that works with the Internet as a global infrastructure is really difficult and involves a lot of engagement with all of the stakeholders. It involves understanding who the stakeholders are. It involves getting those stakeholders to respond.

So the risk that I would see is that urgency and desire to move forward with regulation see that sort of consultation getting lost and result in ill-fitting regulation.

PARI ESFANDIARI: Elena, you have a comment?

ELENA PLEXIDA: Thank you so much, Pari. Yes, following on what Chris was saying now but also before and to your question. I think that [the issue] going forward is the politicization of the DNS and the politicization of the unique identifiers. It makes perfect sense that the governments are making regulations that are real problems on the Internet. But what we see that's a little bit different now is there is a politicization of the foundation of the Internet [inaudible] either with the ideas that there needs to be control over it although technically it works or other sort of ideas that can be [inaudible]. I think it's an issue.

PARI ESFANDIARI: Thank you very much. Olivier, I want to turn the floor to you. We are short of the time. I apologize. It's my fault as the moderator.

OLIVIER CRÉPIN-LEBLOND: Yeah, I know. I was going to ask just one last question to Lucien because he went through such a list of things that the French government had moved forward with and with the outcome and so on. And the question was, how much does all this cost and who's going to pay for it? Sorry for asking it, but obviously….

LUCIEN CASTEX: Thank you. Thank you, Olivier. That's quite a difficult question, indeed. There is no single answer, obviously. And indeed, there is a number of legislation at the French level and also at the EU level, as you know, and more is most likely coming. If I'm reflecting a bit on the issue, I'd say we need to mostly likely promote diversity and recognize each actor in its role. You know, not impose a one-size-fits-all approach to everybody and so everyone could actually have its role implemented. That's in my opinion one of the key takeaways of the French presidency and current debates going.

OLIVIER CRÉPIN-LEBLOND: Right. Thank you so much. I know that we had Seb in the queue. I just asked him to make his point or ask his question on the chat because we are bound by very sharp cutoff times, and we only have one minute.

I wanted to thank all of the participants in this discussion now. The people who have taken part in this and that are in the room and following us worldwide have learned a few things about where Europe is going.

Yeah, Sebastien, you can actually have the last word because it's an idea of Sebastien Bachollet who started this dialogue and this discussion since France was and is at the moment having the European presidency. Over to you, Sebastien. But please make it brief, otherwise we'll get in trouble.

SEBASTIEN BACHOLLET: Thank you, Olivier. To be brief I will not change language. But first of all, I would like to thank you all the participants and the speakers and the organizers, Pari and Olivier. Well done.

I just wanted to remind you that on Thursday we will have another EURALO session or a session organized by EURALO to say the least. It will be about Internet governance and multistakeholderism in time of emergency. And some of the topics you discussed today will be resonating in the discussion we will have in two days, and you are all welcome to participate. I guess it's in this room at 9:00 in the morning here European time.

And once again, thank you very much for these very interesting exchanges. And we will try to follow on that. It's not because France is [leaving] the presidency but it will not be still a topic for EURALO and for Europe to follow what is happening. And in our monthly call we will try to come back to the topic. Once again, thank you, everybody. Have a good rest of the day and rest of the ICANN meeting.

OLIVIER CRÉPIN-LEBLOND: Thank you, Sebastien.

PARI ESFANDIARI: Thank you.

OLIVIER CRÉPIN-LEBLOND: Pari, you can close the room.

[END OF TRANSCRIPTION]