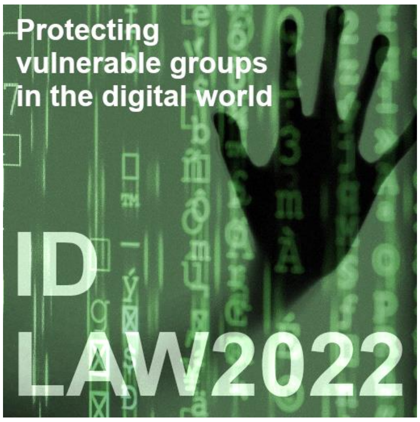
Conference on Innovation and Digitalisation in Law 2022

Résumé



Edited by Peter Hübelbauer

universität wien

Institut für Innovation
und Digitalisierung im Recht

Table of Content

For this year's Conference on Innovation and Digitalisation in Law 2022, we came together to discuss the topic of "Protecting vulnerable groups in the digital world".

The conference took place online on November 9th 2022 from 9:00 to 12:00, Vienna Time (CET) and was streamed live.

The recording is accessible on YouTube via the following link:
https://www.youtube.com/watch?v=XEe-I2qZ41Q

Vienna, December 2022

Speakers & Panelists

Abog. Mariana A. Rissetto, LL.M.
Speaker

Abog. Rissetto, LL.M. graduated from the University of Buenos Aires with the Argentinian law degree Título de Abogado (Title of Attorney) and holds an LL.M. in International Legal Studies from the University of Vienna. Her research interest includes data protection, AI, and new technologies. Since 2019, she has been working on several research projects in the Department of Innovation and Digitalisation in Law, one of which is Privacy4Kids.

Dr. Karl Gladt
Speaker, Panelist

Dr. Gladt is significantly involved in dispute resolution and consumer advice. He worked as a lawyer and is now head of the legal department of the ÖIAT and project lead of the "Internet Ombudsstelle". ÖIAT promotes the competent, safe and responsible use of digital media. Dr. Gladt provides ongoing legal support for various projects of ÖIAT, such as "Watchlist Internet", "Safer Internet", and "digitaleSenior:innen".

Mag. Erich Moechel
Speaker, Panelist

Mag. Moechel is an award-winning journalist at FM4. He focuses on net policy issues. Previously, he worked as an editor at Futurezone, the former IT news website of ORF. Mag. Moechel has many years of professional experience on the topics of surveillance and data protection with a focus on the EU. Just as with the proposed EU Regulation on the prevention and combating of child sexual abuse, he critically follows the legislative processes of the European Union in these areas.

Mag. Joerg Heidrich
Panelist

Mag. Heidrich is a lawyer specialised in IT law, a certified data protection officer and data protection auditor. In addition to his own law firm, he also works for the publisher "Heise" and is known for his podcast "Auslegungssache" at the computer magazine "c't". Heidrich has published many articles in various journals, such as "Spiegel Online", "Heise Online", "Multimedia & Recht" and "Computer und Recht". He is a member of the German Press Council and other associations, like the "Gesellschaft für Freiheitsrechte e.V.".

Dr. Veronika Nagy
Panelist

Dr. Nagy is an Assistant Professor in Criminology at the Law Department of Utrecht University and an International Research Fellow at the University of Milan. Her research interest includes surveillance, digital inequality with a focus on the connection between mobility and technology, criminalisation and digital self-censorship. She has conducted research on specific forms of securitisation, financial surveillance, ethnic mobility, human trafficking and digital profiling, in particular the trafficking of children.

Mag. Sebastian Öhner
Panelist

Mag. Öhner has been a legal officer at the Wiener Kinder- und Jugendanwaltschaft since April 2021. He studied law at the University of Vienna and the Istanbul University. He has been associated with the Vienna Children's Friends in the area of children's rights since 2015. Mag. Öhner is the Secretary General of the League for Human Rights of the Austrian League for Human Rights, with an emphasis on children's rights.

Univ.-Prof. Dr. Christiane Wendehorst, LL.M. (Cantab.)
Opening Speaker

Univ.-Prof. Dr. Wendehorst, LL.M. has been Professor of Civil Law at the University of Vienna since 2008. Amongst other functions, she is founding member, Immediate Past President (2017-2021) and since 2022 Scientific Director of the European Law Institute (ELI) as well as Co-Head of the Department of Innovation and Digitalisation in Law. At the moment, her research focuses on legal aspects of digitalisation and she has been working as an expert on topics such as digital content, the Internet of Things, AI and data economy.

Univ.-Prof. Dr. Iris Eisenberger, M.Sc. (LSE)
Closing Speaker

Univ.-Prof. Dr. Eisenberger, M.Sc. is Professor of Innovation and Public Law as well as Co-Head of the Department of Innovation and Digitalisation in Law. Her research focuses on innovation and technology law, the protection of fundamental and human rights and the intersection of law, innovation and society. She has wide experience in interdisciplinary research as well as in conducting and participating in nationally and internationally funded research projects.

Univ.-Prof. Dr. Nikolaus Forgó
Moderator

Univ.-Prof. Dr. Forgó is Professor of Law and Head of Department of Innovation and Digitalisation in Law, University of Vienna. Further, he is Head of the LLM-program on information and media law at the University of Vienna. Univ.-Prof. Dr. Forgó conducts extensive dogmatic and third-party funded research for European, German and Austrian clients regarding questions of IT law, in particular data protection and data security law.

Univ.-Ass. Dipl.-Ing. Annemarie Hofer
Moderator

Dipl.-Ing. Hofer is a University Assistant at the Department of Innovation and Digitalisation in Law. She studied Environment and Bio-Resources Management at the University of Natural Resources and Life Sciences in Vienna. In her dissertation, she will take an interdisciplinary approach towards (legal) quality requirements for statistical modelling.

Mag. Peter Hübelbauer, BA
Moderator, Editor

Mag. Hübelbauer is a Research Associate at the Department of Innovation and Digitalisation in Law. He studied media studies and law at the University of Vienna, specializing on IT law as well as criminal justice and criminology. Due to his participation in third-party funded projects, he currently deals with analytic tools in law enforcement.

Organisers

Univ.-Ass. Mag. Nina-Maria Hafner-Thomic

Univ.-Ass. Dipl.-Ing. Annemarie Hofer

Mag. Peter Hübelbauer, BA

Univ.-Ass. Mag. Matthias Klonner

Univ.-Ass. Hande Özkayagan Prändl, LL.M., BA

Abog. Mariana A. Rissetto, LL.M.

Dipl.-Ing. Maximilian Treitler, MA

Summary

The protection of vulnerable groups requires educational, legislative and technical measures.

Educational measures are necessary on two ends, namely for legislators and for vulnerable groups. Legislators need to increase their knowledge about technological infrastructures and their understanding of digital culture to know how and why people are engaging with certain platforms. Otherwise, legislators will stay in the dark about what kind of regulation works and what is impossible to regulate.

Vulnerable groups need to be educated about the dangers of the internet and the possibilities of the web. While elderly people tend to need more knowledge about the possibilities of the web to facilitate their inclusion in modern society, children rather need to learn more about its dangers. Educational measures provide an adequate general protection as they enable vulnerable groups to protect themselves.

Legislative measures can only provide targeted protection and require educated legislators with appropriate knowledge about the affected technologies and user groups. Regulators should refrain from pressing forward to regulate something in the assumption that it will be used much more because it is regulated. Rather, they should only take regulatory action when necessary. Otherwise, they risk overprotecting and excluding vulnerable groups from the digital world or protecting vulnerable groups at the cost of everyone including those to be protected, e.g. by impairing significant security standards such as data encryption or violating fundamental rights. Through ombudspersons as well as by adopting a participatory law-making approach, legislators should be able to learn about which technological aspects and influences from social media on human behaviour need actual regulation.

Vulnerable groups should be able to reach ombudspersons easily and tell them their issues. In turn, such intermediaries may be able to interpret the reported problems and communicate those phenomena to the legislators.

If vulnerable groups were to get the opportunity of taking part in law-making processes that are of major importance for their lives, they could provide first-hand input on what needs legislative protection. An example for such a successful integration is the compilation "The General comment on children's rights in relation to the digital environment" from the Committee on the Rights of the Child.[1] If this participatory approach works at the international scale, it should work even more on a national level. Currently, the heterogeneous youth protection laws in Austria are insufficient to protect the youth in the digital world.

The IT community should collaborate with legislators to find coordinated technical measures that are able to guarantee the effective protection of vulnerable groups. Solo efforts are not helpful both in law and in technology. A close liaison between legal experts and technical experts would provide powerful protection by law and by technology to the necessary extent. Eventually, it is necessary to forge a bridge between the legislative parties and the IT community and extend life-long learning in digital literacy on both ends, the vulnerable groups and the legislators, to protect efficiently vulnerable groups in the digital world.

[1] https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation (last retrieved on 28.12.2022).

Opening

Univ.-Prof. Dr. Christiane Wendehorst, LL.M. (Cantab.) opened the conference. In her opening speech, she explained that the IDLaw Conference is organised by young researches from the University of Vienna's Faculty of Law. She complimented the organisers for choosing an important topic, namely "Protecting vulnerable groups in the digital world". Univ.-Prof. Dr. Wendehorst reminded the audience, that the concept of "vulnerable groups" itself has been challenged as it is said that it is potentially stigmatising and inappropriate for the digital world, because in the digital world, everyone might be vulnerable to a certain extent. She argued that nevertheless, there are certain groups in our society that need special protection, such as minors and people with limited capacities. Hence, it is worth a look on how these vulnerable groups are protected in the digital world across different legal frameworks and legislations, without stigmatising them; but rather empowering them.

Presentations

1st presentation

Abog. Mariana A. Rissetto, LL.M. presented the project "Privacy4Kids",[2] which is a collaborative work of the Austrian Data Protection Authority and the University of Vienna that is financially supported by the European Commission.

This project aims at familiarizing children aged 6 years to 14 years with the topic of data protection and privacy issues through animated and age-tailored educational videos. The project was organised by the Department of Innovation and Digitalisation in Law as a course at the University of Vienna's law school. Within this hands-on project, 30 interdisciplinary students from various faculties of the University of Vienna produced 22 videos in the winter term 2021/22 targeting two age groups: children from 6 to 10 years and children from 11 to 14 years. This course provided an interdisciplinary area where students from various fields had to interact with each other.

Abog. Rissetto explained that the challenge was the visualization of legal knowledge about data protection and communicating this knowledge to children. Her students not only had to consider the law and the legal concepts, but also how to transmit the respective message. For this reason, students from other faculties, such as the Faculty of Psychology, Faculty of Computer Science and students from the teachers programme in informatics as well as the general teachers programme were invited to participate. The students split up in 11 groups to have one group per topic, like "Social Media & Influencer", "Internet & Phishing", "Cookies", etc. After their research on the topic from a legal and educational-psychological perspective, they had to transform their results into a script. On that basis they produced their videos, one for each age group, with the tools "Doodly"[3] and "Toonly".[4] To facilitate the use of these videos in school classes as an educational tool, supporting material for teachers was also created.

This winter term (2022/23), a new class of students develops a card game with a connection to the videos by linking to them via QR codes printed on the game cards.

Various events and workshops in schools testify to the success of this project.

[2] See further: https://www.privacy4kids.at (last retrieved on 28.12.2022).

[3] See further: https://www.doodly.com (last retrieved on 28.12.2022).

[4] See further: https://www.toonly.com (last retrieved on 28.12.2022).

2nd presentation

Dr. Gladt presented projects that share the common objective to promote the competent, safe and responsible use of digital media.

In presenting the project "Saferinternet.at",[5] Dr. Gladt highlighted the results from a group of researchers of the pan-European knowledge platform CO:RE that tried to classify the online risks that children might be confronted with. They created a risk matrix, comprised of four Cs, namely Content, Contact, Conduct and Contract:[6]

- "Content" includes harms done to children by encountering disturbing content (e.g., graphic violence, pornography, disinformation),
- "Contact" encompasses risks arising when a child is confronted with a harmful adult (e.g., excessive surveillance, cyber grooming, ideological persuasion),
- "Conduct" covers situations where children are exposed to a harmful peer group (e.g., cyberbullying, sexting, self-harm or other peer pressures) and
- "Contract" includes situations where children are challenged by harmful businesses (e.g., identity theft, issues arising from algorithms and social media).

Dr. Gladt stressed that this is an attempt to categorize the diverse problems children are exposed to. Further, he highlighted the existence of crosscutting issues that emerge in all fields; an example for this being privacy violations.

The project "Saferinternet.at", the slogan of which is "Better Internet for Kids", launched in 2005 and is based on a programme of the European Commission that aimed to establish in each Member State a "Safer Internet Centre". These centres are based on three pillars: Awareness, Helpline and Reporting of illegal content. "Saferinternet.at" organises about 2500 workshops per year in schools, youth centres etc. and distributes information as well as educational material, which can be ordered online and is destined to be used in class. Moreover, this project provides online content like video tutorials and guidelines on how to configure privacy settings in social media.

Another project of the ÖIAT is "DigitaleSenior:innen",[7] which is a service contact point that addresses elderly people with the objective of enhancing the digital literacy of seniors. The project started in 2017 and has so far identified five main categories in which elderly people are vulnerable due to their lack of digital literacy.
Since an increasing number of bank branches is closing, people are getting increasingly dependent on e-Banking. This has a major impact in small towns on elderly people who show scepticism to this trend and online banking. While elderly people are too afraid of the internet and hesitant to use e-Banking, young people should be more afraid of the internet because they might disclose too much private information about themselves.

[5] See further: https://www.saferinternet.at (last retrieved on 28.12.2022).
[6] Children Online Research and Evidence. (2021*). CO:RE Theories Webinar: Understanding online risks for children*. Page 24. Available at https://core-evidence-eu.s3.amazonaws.com/documents/speaker-presentations-pdf.pdf (last retrieved on 28.12.2022).
[7] See further: https://www.digitaleseniorinnen.at (last retrieved on 28.12.2022).

Dr. Gladt explained that the project team also saw in the context of e-Government, that during the Covid-19 restrictions, such as the lockdowns, elderly people encountered issues like getting the Green Pass, or providing the digital signature.
Further, elderly people are most susceptible to online fraud. Dr. Gladt gave an example of a tech scam, where people are called by alleged Microsoft support teams and then grant access to their computers and their sensitive information. Elderly people also tend to fall more easily into a love scam, where they believe in a relationship that is fake and transfer money to fraudsters.
Due to their lack of digital literacy, elderly people suffer disadvantages in e-Commerce as many have a worse access to lower prices or know how to consult and compare online reviews.
Lastly, elderly people have difficulties to interpret information on social media correctly, because they are used to classic, edited media. With a lack of media literacy, they have a limited access to information. Dr. Gladt also briefly addressed problems coming from Ambient Assisted Living (AAL), which includes surveillance issues and interference in private autonomy.

To tackle these problems and to enhance the digital literacy of elderly people, this project supports educational institutions in planning and implementing digital training for seniors, following the logic of "train the trainers".

In the context of the project "Internet Ombudsstelle",[8] which resulted in the setup of an Alternative Dispute Resolution (ADR) in e-commerce and other disputes, Dr. Gladt highlighted that especially young people are less likely to seek advice in the traditional way. Rather they seek advice from online sources. To facilitate this, the ÖIAT provides information about dispute resolution on the website of the "Internet Ombudsstelle". As they have already received many complaints and advice requests regarding fraud and online scam after the damage was done, the ÖIAT launched a spin-off called "Watchlist Internet"[9] in 2013. This project aims at preventing damage by raising awareness about fraud schemes, through their website where they offer up-to-date news about online fraud and fakes. The underlying concept of this website is to give everyone the opportunity to check whether an online shop is fake, before they order something online. Therefore, the "Watchlist Internet" is search engine optimized, to appear among the very first search results, when someone enters the domain of a webshop in a search engine, such as Google. In order not to depend solely on user reports of suspected fake shops, the ÖIAT started to develop a fake shop detector together with IT experts from the Austrian Institute of Technology (AIT) and with developers from X-Net, by using Machine Learning based on code snippets of fake shops.[10] This application is an internet browser plug-in that indicates the fake shop probability via a traffic light system.

☝ The audience asked Dr. Gladt, what a mandatory education of seniors could look like, if we want to prevent further harm to this group.

Dr. Gladt responded that it could look like a digital driving license, but he thinks that such measures would be incompatible with fundamental rights and therefore it would not be a viable way to make

[8] See further: https://www.ombudsstelle.at (last retrieved on 28.12.2022).
[9] See further: https://www.watchlist-internet.at (last retrieved on 28.12.2022).
[10] See further: https://www.fakeshop.at (last retrieved on 28.12.2022).

education mandatory. It would rather need measures to make education more attractive and to make clear to elderly people that they miss out many things if they do not use digital media. Such educational measures should be implemented by providing ongoing training that is tailor made for elderly people, e.g. introducing digital officers in homes for the elderly.

3rd presentation

After a short break, Mag. Moechel presented the proposed EU Regulation on the prevention and combating of child sexual abuse (CSAR).[11] He introduced this legal instrument as an example of "how not to protect vulnerable groups".

In his view, this proposal introduces mandatory data mining obligations, which are presented as a measure to protect the most vulnerable of all: children who are frequenting the internet. Mag. Moechel described these legal measures as a false flag operation. He stated that he has been following the making of this proposal since 2014 and that he has addressed these developments in about 60 articles.[12] According to him, 85% of the web traffic was not encrypted until 2013, allowing all intelligence services to easily tap the wires, in particular at the internet exchange points. The Snowden revelations from 2013 led to the general encryption of internet traffic.

Mag. Moechel said that in 2015, already 65% of web traffic was encrypted. This means that the intelligence services have lost one of their most valuable assets in being able to track anything on the net. He continued that in 2014, the EU worked on the first proposal to introduce "Golden Keys" for security services and police to provide them with an alternative point of access to read the encrypted data. Since then, there have been many anti-encryption campaigns. To give an example, Mag. Moechel referred to the proposed mandatory filtering due to terrorist content online, which was put forward by the EU in 2016. Such proposals, however, have not been transformed into regulations thus far. He concluded that the first obligatory content filtering passed the EU Parliament in the context of copyright law with the DSM Directive in 2017.

Mag. Moechel proceeded in saying that the EU is trying to implement data mining and artificial intelligence in all fields today, including risky fields. Following his assessment, law enforcement and security lobbyists try to achieve the same decryption results with the proposed CSAR today as they have tried to since 2014.
In this context, Mag. Moechel strongly criticized the plans of the EU to establish a new agency against child abuse on the premises of Europol that already has much experience in data mining. This new EU centre against child abuse shall be empowered with competences that EU parliamentarians refused to grant Europol in June 2022. Hence, another agency, under the same roof, would use more or less the same technologies as Europol under a mandate, which allows the new agency to use methods that Europol is not allowed to do, Mag. Moechel stated.

[11] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (COM/2022/209 final).
[12] See further: https://fm4.orf.at/tags/erichmoechel (last retrieved on 28.12.2022).

Further, Mag. Moechel criticized the constant misinformation and bad political style, in particular from EU Commissioner Johansson, who, according to him, used marketing numbers from Microsoft and claimed that the used AI methods will get 90% hits. Mag. Moechel argued that the opposite is true, as random and inconsistent data sets produce many false positive hits. This would lead to harmless content being searched, as the algorithms have found some similarities (e.g., a picture of a child and a man in swimming trunks on the beach).
He accused Ms Johansson for using manipulated and wrong numbers when she claimed that the depictions of child abuse had risen drastically since 2016. According to Mag. Moechel, the reason for this is rather technical, as in the past the analysis of the hash values of videos was not fully developed, but only those from images. Since 2016, software has been capable of understanding and hashing video content. That should be the reason for the enormous increase in numbers depictions of child abuse.
Mag. Moechel added that another – much-underestimated – factor for the increase is Sexting. In Germany, around 40-45% of the perpetrators of "child pornography" are children and very young adults. They are not comparable to actual perpetrators.
Hence, according to Mag. Moechel, the legislative process of CSAR is based on incorrect figures and wrong assumptions.

He argued that before the legislators started the process for this proposal, they would had needed data retention and mass surveillance already in place, but the EUCJ invalidated data retention in 2014 and reaffirmed in multiple verdicts over the past years that data retention is illegal for big data analysis.

Mag. Moechel stated that he finds it incomprehensible how the Commission could make this proposal. In his opinion, it is either a high level of ignorance he has never experienced before or a deliberate move to fulfil what the Commission had told the Council in 2016 that the police would get new instruments for policing. Following Mag. Moechel, the EU proposes a regulation to protect children that simply will not work.

He said that for every surveillance proposal he has been hearing for the past 28 years the same catch phrases, which are either starting with "child pornography" or terrorism. He reminded the audience that even the first legal basis for the police to access phone calls and GSM records was reasoned within the EU under the flag of child abuse and terrorism.

Mag. Moechel explained that he sees other ways to protect children, like a mandatory year early in school so children would understand the dangers of the internet.

Panel discussion

Mag. Heidrich started the discussion by adding to the last presentation child pornography should rather be called "child sexual abuse material" (CSAM). In his view, this proposal is another attempt of the EU Commission, where they are trying to build up surveillance of any kind of electronic communication, including telephone, email, messengers (including video game chat, dating apps, video conferences, etc.).

Mag. Heidrich enumerated some threats to privacy from the proposal:

- All this communication should be monitored by some policing agencies, or by some agencies close to the police.
- There is a plan to break up encryption. End-to-end encryption messengers will have to be opened to give law enforcement the possibility to access their contents.
- It is planned that hosting services should be scanned regarding web postings, social media, video streaming, file hosting and cloud servers.

Mag. Heidrich concluded that it looks like the whole internet will be scanned in the future if this proposal enters into force. There would be automatic scanning of images, videos and text. Mag. Heidrich stated that this approach may work with images, but not with texts, as anything suggestive of CSAM will be reported. Mag. Heidrich agreed with Mag. Moechel that there are way better ideas for protecting children. He supported Moechel's assessment that CSAM would only be the first step for the implementation of more surveillance measures. Mag. Heidrich said this would open the Pandora's Box and the next steps would likely be the use of copyright law to scan everything on the internet for copyright infringements as another justification for surveillance measures.

☝ A question from the audience was whether the proposed CSAR is not unlawful if already the European Court of Justice ruled in September 2022 that traffic and location data of EU citizens may only be stored in cases of a serious threat to national security. The question referred to the mass data retention of Germany's Telecommunications Act.

Mag. Heidrich answered that there is a high chance that it is not legal. There has been an analysis from the German constitution blog,[13] which is quite well known, in which the authors argue that the European and the German constitution most likely do not cover this proposed Regulation.

Mag. Moechel and Mag. Heidrich agreed that this does not stop the Commission from doing this. In his opinion, the fact that the EU is trying to find technical solutions to social problems is the main problem in these times.

☝ Another question from the audience was how to determine and verify characteristics that require protection, i.e., how to verify a person's age and identify people who use certain services to protect them.

Dr. Gladt answered that this is a sensitive topic and that such an approach may lead to the permanent surveillance of users on the internet. He thinks that as soon as a system of eIDs is in place, there could be data protection-friendly ways to verify the age of users, without requiring users to provide more information than the eID. He specified that there would be the restriction of jurisdiction though, leading to the problem that even if providers were obliged to implement such age verifications, they would not be subject to the jurisdiction anymore as soon as providers decide to move their seat to somewhere else.

[13] See further: https://verfassungsblog.de/tag/chat-control (last retrieved on 28.12.2022).

Mag. Heidrich added that the EU's plans on chat control include mandatory age verification for communication and storage apps, as well as for app stores. He explained that such a mandatory age verification would end anonymity, at least in this part of the web.

Mag. Moechel said that there are two ways to verify a person's age. One is to hand over some kind of ID card. By doing this, one hands over sensitive data to commercial networks, such as one's age and name. The other one is the use of eIDs, which will always involve the state. However, eIDs would lead to a user profile encompassing all interests of a user who visited sites that demand age verification. Therefore, either private entities or the state will collect additional data attributed to an existing profile. Mag. Moechel warned that this is a danger to everyone's privacy and one should not hastily introduce such verifications.

Mag. Heidrich continued by addressing children's use of social media. He sees much negative influence coming from influencers, in particular on TikTok. Heidrich is astonished that there is no regulation regarding TikTok, at least in Germany. Currently the only regulation addresses merely the mandatory disclosure of marketing activities. He gave an example of negative influence of some influencers who flew to an island, where they basically told their audience that going outside to enjoy the sun helps against depression and that they should wear sunglasses of a specific sponsor.[14]

Univ.-Prof. Dr. Forgó stated that this was a beautiful example to show how extremely important it is for lawyers and lawmakers to have an idea of what is happening in the digital world. Currently, such issues are something no one is interested in and nobody dealing with the legal implications is really into it.

Dr. Gladt gave a further example of the negative influence of social media, in which people with eating disorders grouped together, but instead of helping each other to tackle their problems they accepted challenges that made it worse, because those challenges encouraged them to lose more weight. Dr. Gladt believes that such dangerous practices have to be regulated in some form and not left to the market. He said that public authorities need to intervene, but it is difficult to draw the line between influencers' marketing practices and their implicit encouragement of harmful behaviour.

Mag. Öhner suggested that children and young people need to get the opportunity to participate in the debate on regulation. According to him, legislators need to bring in the people who are on these platforms and hear their voices, because from a children's rights perspective, this is very important. He claimed that this also works on an international level, and referred to "the General comment on children's rights in relation to the digital environment" from the Committee on the Rights of the Child,[15] which was created with children in a participative manner.

Regarding influencers, Mag. Öhner is also dealing with "kidfluencers", children who are influencers themselves. Although child labour is prohibited in Austria, "kidfluencers" have many followers on

[14] A similar example available at: https://twitter.com/JSchmitzLeipzig/status/1590949967501430784 (last retrieved on 28.12.2022).

[15] https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation (last retrieved on 28.12.2022).

different platforms, earn much money and have contracts in place, but without any regulation of children's rights behind them. Mag. Öhner argues that our legal systems and child labour laws are not able to deal with to these particular issues.

☝ A question from the audience was how we could ensure that well-meant protection measures do not simultaneously eliminate the ability of vulnerable groups to participate in our society, meaning not to exclude them by overprotecting them.

Mag. Öhner answered that we need to find the right balance between the protection and the participation of children and young people. The digital world is very important for children, so one cannot just ban them and overprotect them in a way that results in their exclusion. Mag. Öhner said that legislators need to seek the fields where protection is necessary and then find out how far the protection has to go, but always from a participative standpoint. He stressed that the educational aspect is important: If children are educated about their rights and the laws that are relevant in the digital world, they will be able to navigate within these boundaries and can protect themselves. Additionally, it is also necessary to focus on the aspects where children need to be protected. Mag. Öhner mentioned as an example that children are easily exploited in online games with in-game purchases and spend a lot of money. Moreover, such games are also very addictive and there is social pressure. In these cases, we need not only protection by education but also the law that protects children from getting into such contracts.

Mag. Heidrich said that he has several cases in his law firm dealing with in-app purchases of the amount between 5.000 – 10.000 Euros. In one of these cases, a 7-year-old spent on in-app purchases 30.000 Euros.

In Dr. Gladt's experience, this does not only happen to children, but also to elderly people. Dr. Gladt had a case in which an elderly person was shopping online, but no longer knew what she was doing. Her daughter had to cancel many orders and asked what she could do about it, and how she could restrict her mothers' harmful e-commerce behaviour. Dr. Gladt said in order to protect those vulnerable groups, one might have the legitimacy to limit their ability or capacity to bind themselves to agreements.

Dr. Nagy added that we tend to think in a very protective way about any kind of vulnerable people. She has been working with minors, ethnic groups, refugees, and people in different gender positions, who would construct the idea of vulnerability in different ways than we do through the law. Therefore, she suggests to always consider the context and the kind of vulnerabilities we define and associate with each group when we are talking about vulnerabilities.

Dr. Nagy observed that in many discussions users, who are social individuals, are called data subjects. Hence, she argued, it is important to differentiate between the information that has been shared through particular infrastructures and devices about this person and if this person is really the person who has been associated with that data (regardless of whether it is about private data, personal data, or regular data etc.). She suggested that such a kind of detachment would help to understand who is standing where in this kind of vulnerability discussion.

Further, Dr. Nagy highlighted the imbalanced relationship between the markets and authorities. She noted that legislative parties often lack both knowledge of the technological infrastructure and a digital cultural understanding of how and why people engage with certain platforms. Dr. Nagy indicated that when the role of large corporations in shaping the digital market is discussed, one needs to keep in mind that public authorities are also dependent on the services and technologies that many of these corporations provide. Therefore, she argued, one cannot detach from this kind of stakeholdership in terms of accountabilities between public and private anymore. She said that even civil societies often engage in the surveillance of vulnerable groups, e.g., the UNHCR practices regarding refugee applicants.

Dr. Nagy stressed that we need to pay attention to three things in particular:

- First, the socioeconomic context where users are identified as vulnerable.
- Second, the distinction of the kind of media literacy that one thinks is essential when discussing education and how people should be taught certain skills in using the internet.
- Third, in law enforcement and policymaking we need to be very careful not to engage in CCC - the control-conform-and-collect approach: the more data we have, the more control we exercise, and the more conformity we should provide for the user community in different digital contexts.

Dr. Nagy explained that she sees a threat in the reproduction of the old paradigm of profiling, which originates from traditional police science. She argued that this strong policing approach does not lead to any engagement with the digital transformation of society. Rather, an anticipatory approach to managing these types of transitions is required, Dr. Nagy suggested.

☝ A question from the audience was how we can tackle the highly addictive potential of social media platforms.

Mag. Öhner answered from a children’s rights perspective, that social media platforms want especially young people to stay attached to their services. He said that there needs to be more awareness about the dangers of using them. He referred to the video shown in the Privacy4Kids presentation and argued that such videos contribute to helping children understand how to deal with the digital world and its dangers, such as addiction. Mag. Öhner shared that he helps parents how to work with their children by explaining to them how much time they can spend on a particular website and by motivating them to keep track of their time using their phone on their own to increase awareness of addiction. Again, he stressed, this shows the importance of the educational way within families and working with children.

Regarding the regulatory perspective on social media platforms, Univ.-Prof. Dr. Forgó referred to the recent large exodus from Twitter that led to the rise of Mastodon. He said that Mastodon is very different from Twitter for many reasons, but mainly because it is rather a protocol than a platform. In his view, this is very interesting and reminds him of the old days of the internet. Univ.-Prof. Dr. Forgó asked the panel if this exodus from Twitter is an example of how legislation has a very high risk of missing the point, either because lawmakers don't properly anticipate what will happen, as in this case, or because they are years behind. Further, Univ.-Prof. Dr. Forgó asked if it requires more communication with IT professionals and more debates about technical protocols instead of discussing laws, legal cases, and legislation.

Mag. Heidrich said that he cannot think of any benefit of legislators trying to regulate technical ideas, especially if the legislator is stepping ahead in the assumption that everyone is going to use something if it is regulated. He rather prefers legislators that only regulate if they have to and do not go ahead.

Dr. Nagy drew a comparison to language; she put forward that many support the idea that there should be laws and regulations about what is correct and what is acceptable in terms of using language. She argued that the very same kind of innovative organic nature of development and change are the characteristics of the technological infrastructure as of language. In her view, one cannot just restrain or discipline it like other kinds of analogue structures. Dr. Nagy suggested that it needs consideration from what perspective one is looking at stakeholders and what kind of behaviour one wants to regulate.

Mag. Öhner agreed that one has to consider how the law should ensure child protection in the digital world. He argued that in Austria are nine different youth protection laws, one for each of Austria's provinces, with the objective of protecting children not only in the real world, but also in the digital world. Mag. Öhner explained that they work in the analogue world, but they are far away from protecting the youth in the digital world, as there are no effective measures for their execution and enforcement in the digital world.

Univ.-Prof. Dr. Forgó continued that he thinks that people that have digital skills are able to circumvent certain paradoxical laws and predictions coming from legislators. In his opinion, children or elderly people, however, lack such skills. Univ.-Prof. Dr. Forgó argued that they simply fall through the cracks as the legislator does not really meet their needs and they do not have the skills to help themselves. He asked the panel if it is up to the legislator or to the legal profession to find some tools similar to consumer protection. Univ.-Prof. Dr. Forgó continued asking, whether it needs ombudspersons, or lobby groups to help those marginalised groups to make themselves better heard or if they should educate the legislators and tell them what can be done and what is to be avoided.

Mag. Öhner addressed this question by pointing out that in the children's rights they have the PPP rule, the provision-participation-protection rule. He said, these three aspects should always be in place from a children's rights perspective and explained that "provision" means one has to provide laws, which have the best interest of the child always in their centre, whereas "participation" means that one lets children and young people participate in every part of the law-making process.

Mag. Öhner referred to the Austrian constitutional right of every child to participate in every aspect that is important for this child. Therefore, from a regulatory perspective, children and young people need to be part of law-making processes that are of significant relevance to their lives, he argued. He stressed that this way, they can give input where protection is needed.

Mag. Öhner explained that the benefit with children is that they are within the school system, where mandatory digital education can be introduced to educate them on how to act in the digital world and he believes this is a very important part of protecting and empowering children in the digital world. From a regulatory perspective, Mag. Öhner suggested that we need to decode the best interest of the child in the digital world for every law-making process and set this as a standard.

Mag. Heidrich said that he used to hear several times in Germany the intention that there should be education about digital devices, about digital development, or about the dangers of social networks, or social competence to detect fake news etc., but nothing is really happening. In his view, only a few very good people go to the schools and do workshops. Mag. Heidrich asked, if this is actually happening in Austria, or if it is still a "should" like in Germany.

Mag. Öhner answered that he thinks that the platform "Saferinternet.at" is a good example of how education in the digital world for children can work. Mag. Öhner noted that digital literacy is an increasing educational aspect in schools in Austria. He observed that they are focusing more on digital learning in schools, but this also brings problems as not everyone has equal access to the digital world. As an example, he mentioned that during the Covid-19 pandemic schools had to switch to online schooling and some children just did not have any notebooks or access to the internet. Mag. Öhner believes those children got lost within the educational system for quite some time. He concluded that when it comes to working with digital possibilities, the question is who is supposed to give children access to the digital world.

Dr. Gladt came back to the question of Univ.-Prof. Dr. Forgó, whether it needs education, regulation or something different to make marginalised groups better heard and to provide them protection. Dr. Gladt said that all of it is required, as not only the digital literacy of people needs to be enhanced, but also at the same time, it needs some sort of regulation to start holding platforms more and more liable for what is occurring within their respective sphere. Dr. Gladt reflected that regulating digital gatekeepers could also be a more cost-effective approach, and this could be the reason why the legislature decided to take this approach. Further, he expressed that those ombudspersons or ombuds services are necessary as some kind of seismograph to know what is happening on the web, what kind of questions people have and what issues they are dealing with. Dr. Gladt thinks that one has to keep the threshold for asking such questions or filing complaints as low as possible. He explained that this can be achieved with ombudspersons offices, which ought to try to interpret those phenomena and communicate them to the regulators so on that some sort of action can take place. Dr. Gladt doubted that education alone would be enough.

Mag. Heidrich agreed to the need for regulation, but he narrowed down that it must be done carefully and must not curtail fundamental rights.

Dr. Gladt concluded that communities should not be too opposed to any kind of regulation. He stated that there is a tradition in the IT community to reject any kind of regulation or proposal and suggested that it would be rather constructive to participate or contribute to finding a fair balance in order to achieve objectives such as protecting vulnerable groups.

Closing

Univ.-Prof. Dr. Iris Eisenberger, M.Sc. (LSE) closed the conference. In her closing remarks, she stated that the protection of vulnerable groups is often not adequately regulated within European Union law. She argued that not only the lack of digital natives in the EU's hierarchy is one of the reasons, but also the lack of adequate legal competences. Univ.-Prof. Dr. Eisenberger said that rather most of the EU legislation is internal market driven as well as safety and security driven, often leaving aside other important issues, which is also true for the draft of the EU Artificial Intelligence Act.

Univ.-Prof. Dr. Eisenberger thanked the organising team for all their work they put into this conference, all speakers and panellists for their time and great input, and all participants for their engaging and interesting discussion online. Lastly, she thanked Univ.-Prof. Dr. Nikolaus Forgó for providing the room and the environment to have these kind of critical and much needed interdisciplinary discussions.

Do you have any comments?

Reach out to us via idlaw-conference.id@univie.ac.at