In this TATuP interview, Georg Plattner talks with Matthias Quent about his research on the metaverse in the Immersive Democracy project. In order to shape the emerging virtual reality-enhanced internet of the future in a way that is conducive to democratic coexistence, we must also try to prevent possible malevolent uses. This presupposes that key actors such as technology developers, civil society, and the state work together to shape immersive realities and draw the right conclusions in order to negotiate viable compromises in the conflict between opportunities through innovation and social risks for democracy. Last but not least, it is important that there is also room for genuine democratic community in the future digital space.

Georg Plattner: What is the background to the Immersive Democracy project? Can you explain how the project came into being, what it is about, and what the whole thing has to do with malevolent creativity?

Matthias Quent: I spoke with Meta and suggested that in order to develop the internet of the future with the metaverse, then we also need to look at how the security of democratic communication and democratic culture can be ensured and take responsibility for this. Following this, a project was initiated as part of the European Metaverse Research Network. The aim is to analyze the internet of the future, discussed under the term metaverse, in order to learn from the mistakes and vulnerabilities of Web 2.0, the social internet, and to prevent them in the future. In other words, how can a metaverse, how can immersive virtual environments be designed to be conducive to democracy, or at least not detrimental to democracy? It is therefore important to also consider aspects such as possibilities of immersive technologies, by three-dimensionality, but also by aspects of presence and persistence, so that a kind of parallel world exists, at least for a certain part of life.

The metaverse or immersive realities are still dreams of the future. What do you see as the lessons learned from Web 2.0 in the project? What risks do you see for immersive realities or for the internet of the future if we fail to learn from the mistakes of the past?

This has several levels and relates to different use cases. In the gaming sector it is different than in the social or industrial metaverse. We generally have to differentiate between problems that already existed or are noticeable in a very similar way in Web 2.0 and potential new problems. The former are generally expressions of hate speech, radicalization, instrumentalization, micro-targeting, everything that can be used by malevolent actors. How might this continue in immersive environments? The second is: What specific new aspects come into play, for example, when it comes to a direct verbal exchange, rather than via the written medium? What if it is also about AI-supported questions of generating environments or generating interaction, and thus even more about manipulation possibilities? Our project focus, also based on our experiences in recent years with polarization and radicalization in the political sphere, is particularly on aspects of dealing with radicalization actors, with hate speech, but also on certain mechanisms that may have implicit effects, such as algorithmic emotionalization or the creation of filter bubbles. In my opinion, the latter can become even more of a problem in the metaverse than in Web 2.0. Such filter bubbles, which we know do not currently exist in the form and quantity suggested, are much more realistic in the metaverse. We see this in the empirical research that we conduct to a limited extent on virtual realities. There, users show a tendency to simply block avatars or other people who irritate or disturb them. This is seen as a panacea, but it also leads to the creation of these sepa-

Keywords - metaverse, malevolent creativity, immersive worlds, virtual reality, democracy
rate worlds. This not only raises questions about the technological infrastructure but also about the effects this has on personalities and society. Will this increase singularization even more dramatically than we have already discussed and seen empirically? On the other hand, a closer look reveals that much of the radicalization and polarization taking place in Web 2.0 is also fed by the fact that we are constantly confronted with others. It is easier to avoid this in virtual immersive environments. On the other hand, however, it can be assumed that the impacts and consequences of harassment or some form of attack, for example, will be even stronger there, simply because the intensity of the experience, for example, through some form of augmented reality, has a stronger cognitive and emotional impact.

Have you already been able to gain experience in your project with the new technologies relating to the metaverse? There are already experiments with virtual reality in the gaming sector, for example. Are there cases where malevolent actors have actually used these metaverse-adjacent technologies creatively for their own purposes?

In the project, we work decentrally with stakeholders and experts from various civil society and academic fields. A study by the Amadeu Antonio Foundation took a very close look at the gaming sector. In the gaming sector, we are already most likely to see something like a metaverse in terms of 3D environments, a high degree of immersiveness, and interaction. There are all sorts of attempts to use this, from custom-programmed worlds such as concentration camps or places of terrorist attacks that are recreated on Roblox to spam in chat. This happens at a low-threshold level and is difficult to measure because it tends to happen organically and is not necessarily integrated into larger campaigns. Extremism researcher Julia Ebner has looked closely at what happens or can happen in so-called DAOs, that is, digital autonomous organizations. These show a high degree of resilience to repression, to banning, or to any form of intervention against radicalization. But actually she hasn’t found too many concrete activities at the moment. There are the indicators, there is the technology, there are the trends, but due to the relatively low number of users and the high technical requirements, this is still more for early adopters. At the moment, it can still be designed and observed. These are not yet large-scale spaces for radicalization like certain channels on Telegram.

Let’s start with the developers, who should or do have a vested interest in creating safe environments and at the same time, of course, given that they are driven by commercial interests in particular, have a contradictory relationship to this because everything that stimulates, that perhaps also leads to polarization, is potentially also a stimulus for these spaces. In my view, developers first need to be aware that there is this risk of misuse and that this risk of instrumentalization is relevant because it leads to different conclusions. On the one hand, this concerns the design. Especially in the virtual space of the metaverse, many questions arise, starting with “How should avatars be designed? What skin colors can avatars have? Is this discriminatory or is it not discriminatory? What gender identities?” through to “Can extremist symbols – swastikas or other symbols, which are often also codes such as the white power symbol or other symbols – be used? Are they allowed or are they already technologically prevented and filtered out?” Above all, however, the question is – and this is not so different from Web 2.0 – how responsive is the platform to complaints? How reflexive are the community standards? How do you deal with it when large swastikas are built in Minecraft worlds, but are designed in such a way that they do not directly contradict the community rules? You can still report them, of course, but it won’t lead to anything. Or the decision-making power is returned to the community, which should then decide on bans. But this puts you in a very difficult position in terms of evidence or justification. In other words, just in this internal relationship, not even talking about regulation or cooperation with security authorities and all that, in my opinion it is important to have proac-

**Such filter bubbles, which we know do not currently exist, are much more realistic in the metaverse.**

I would now like to move on to how we can prevent the mistakes that may have been made on the internet from happening again and how we can preventively counteract malevolent creativity. I would like to focus in particular on three groups of actors: developers, civil society, and the state. What can developers do to make these immersive realities safe?
tive community management in the sense of a democratic culture that strengthens those who oppose toxic tendencies, who report things, and who, in case of doubt, also kick malevolent channels or actors off the platforms. This requires not only easy to integrate with those organizations or communities that are already active in the relevant worlds. Coming in from the outside and saying “We are now doing social work in the metaverse” will probably not work well. You need access to the

**Much of virtual reality is ultimately based on the fact that you can ban people individually. Then you can no longer see someone yourself, but that does not solve the problems.**

the appropriate community standards but also the corresponding technological possibilities. Much of virtual reality is ultimately based on the fact that you can ban people individually: Then you can no longer see someone yourself, but that doesn’t solve the problems.

**How can civil society help ensure the safety of immersive realities?**

I believe that civil society faces the great challenge of understanding what is actually happening and what it means that new technologies and implications are coming our way. That’s why it was so important for us in the project to be transdisciplinary: at least also contribute to the qualification of civil society. Everything that is currently being discussed in relation to AI also plays a role in metaverse worlds and immersive realities. At the same time, especially in the area of right-wing extremism, we have the problem that right-wing extremists can exploit these niches better, faster, earlier, and more intensively than civil society actors. This has actually been the case in all phases of the internet; at the moment, you can see this very strongly on TikTok, and it is very obvious that this will also take place in metaverse environments. This is why we need to first of all understand the problem. Moreover, it’s not that communities and therefore also to other generations. I see this as the core challenge, plus the fact that civil society must put pressure on developers and companies such referring to scientific evidence, but also on its own civil values, and must exert influence on politics to shape, regulate, and support this in a normatively positive way.

This brings us to the third actor, the state.

**Are there any particular challenges in regulating digital spaces?**

The regulation of digital spaces is currently undergoing major changes, particularly as a result of European legislation. I think we first have to accept that social media and social spaces are not limited to very, very large platforms. Decentralized technologies controlled or supported by blockchain, such as those made possible by the metaverse, will lead to much more happening in much, much smaller, more fragmented spaces. Regulators need to understand this too. Then, a series of new legal questions must be answered. Is a death threat against an avatar a death threat against the person behind it or only against the avatar? How is this to be handled legally? There are individual cases and also discussions about this, but in the wider picture, when it also comes to legal enforcement by the security authorities, this is still a black hole for very, very many people.

**Do you have any insights into why right-wing extremists in particular are often early adopters of new technologies who are quick to take advantage of the new opportunities?**

Well, the widespread theory is that they lack the larger channels, that they are denied normal opportunities to participate in the democratic spectrum, in the media, in youth clubs, or other meeting places. However, I believe that this is now only half true due to the mainstreaming of right-wing extremism in recent months and years. In addition, there is the strong manipulative appeal that comes with the technologies, the fact that they can be used manipulatively and thus provide a new basis for potentially totalitarian fantasies. Secondly, this may also have something to do with different internet cultures. We see, for example, that the LGBTQI scene is very adept at using VR spaces for their own purposes, such as for meetings in protected spaces. New opportunities are therefore more likely to be taken up by those who find it difficult or impossible to participate elsewhere. However, it must also be said that much of the discourse on VR technologies and the metaverse among the extreme right or conspiracy theorist groups tends to show a negative attitude. So, on the one hand, there are actors who use this experimentally or from their own living environment – they are just out there, like others are out there, and then they use it for their political agenda. On the other hand, however, they basically declare it to be part of an overarching doomsday and conspiracy explanation, according to which technologies such as the metaverse, neurobiological developments, chips, etc. are actually part of the plan of a global liberalism that aims to abolish and replace humanity and thus make it more exploitable. Maybe this is also one of the reasons why there is a lot of racism and hatred and stuff like that in practice at the moment, but relatively few or almost no organized campaigns.
Finally, two major questions: Firstly, where do you see the greatest risks for democracy and democratic society in immersive realities in this new internet? Where is the greatest potential for democracy and democratic resilience in immersive realities?

In my view, the greatest danger is the loss of community and the possibility of even more intensive emotional manipulation. This means that you actually withdraw from something like society and retreat into small communities where you always choose what you want to talk about and with whom. Anything to the left or right of it or pluralistic does not take place and you can then ultimately escape into a virtual world of harmony that evades the complexity and ambiguity of political reality. This is no longer democratic, but conformist. I see the greatest opportunity for immersive realities in the fact that they can help better understand how other social groups are doing, that they make it possible to slip into the shoes of others and perhaps also generate solidarity. They can also help give previously unreachable groups and actors access to educational content. These are my spontaneous thoughts on it.

Thank you very much.

How meaningful or how critical is it when states or developers are already starting to regulate certain potentially malevolent uses of a technology, for example, by filtering content? How can we ensure that this is still conducive to democratic politics and does not turn into what right-wing extremists or conspiracy theorists might call "censorship"?

This is a conflict where there is no clear opinion. Particularly with such risk-related approaches to regulating technologies that do not really exist yet, there are opposed to certain regulations, which in turn can open up spaces for hatred and radicalization. This is a conflict that, in my view, can only be resolved by engaging with various civil society actors, where possible based on empirical evidence, discussing it, and not defining the rules too narrowly. It’s about finding proportionate solutions based on observed, observable, or assumed problems. Now, of course, as a scientist I have to say: To do so, we need much more research in this area. Our project is a small project, everything we are doing is very manageable. Developments are faster in other countries on other continents, so we need much more knowledge about what is actually happening in order to be able to design regulation in such a way that it does not lead to overblocking or other overreactions but maintains the degrees of freedom that are possible or conceivable and reduces the risks to liberal democracy.

things that are discussed primarily from the point of view of economic innovation and less in terms of democratic politics or democratic theory. This is also why it is so complicated that perhaps the great danger does not necessarily lie in the opportunities for abuse, also by extremist actors, which are desired for reasons of pluralism, but rather in a justified openness to economic competition and innovation that is opposed to certain regulations, which in turn can open up spaces for hatred and radicalization. This is a conflict that, in my view, can only be resolved by engaging with various civil society actors, where possible based on empirical evidence, discussing it, and not defining the rules too narrowly. It’s about finding proportionate solutions based on observed, observable, or assumed problems. Now, of course, as a scientist I have to say: To do so, we need much more research in this area. Our project is a small project, everything we are doing is very manageable. Developments are faster in other countries on other continents, so we need much more knowledge about what is actually happening in order to be able to design regulation in such a way that it does not lead to overblocking or other overreactions but maintains the degrees of freedom that are possible or conceivable and reduces the risks to liberal democracy.

Thank you very much.