REGULATORY CHALLENGES OF IMMERSIVE TECHNOLOGIES

What is it about? (Definitions)

VR or Virtual reality - the computer-generated simulation of a three-dimensional image or environment that can be interacted with in a seemingly real or physical way by a person using special electronic equipment, such as a helmet with a screen inside or gloves fitted with sensors.

In other words, it is a real or simulated environment in which a perceiver experiences telepresence.

AR or Augmented reality - a technology that superimposes a computer-generated image on a user's view of the real world, thus providing a composite view. In other words, AR supplements the natural environment users see around them; it does not completely replace the natural environment in the way that VR does. A real-world environment´s elements are augmented by (e.g., overlaid with) one or more layers of text, data, symbols, images or other graphical display elements.

MR or Mixed reality is a blend of physical and virtual worlds that includes both real and computer-generated objects. It is also understood as an integration of VR and AR.

Potential Negative Impacts (Disadvantages) of AR

AR or ImTe in general can enable cybercrime in a number of areas, including child abuse, virtual groping, cyber assault, stealing of virtual property, illegal betting with virtual money, identity theft, strobe lighting and mere indecent exposure such as nudity, orgy etc.

Users of AR/VR technologies have used it to commit murders, defraud others and even injure themselves (Prajapati, 2018). Some of these cases are rather bizarre, like a VR gamer who was caught for stealing virtual property which apparently possessed huge value in a virtual game called 'RuneScape', by hacking into profiles of other gamers (Prajapati, 2018). A VR gamer sold virtual property for real money in fan forums. He was convicted of hacking into user accounts not of theft (Harbert, 2017).

There are these **security concerns**:

- **Hacking**: especially when a device is synced to a smart watch, smartphone or PC.
- **Data breach**: If the AR system is able to run simultaneously with other applications, this may cause that the voice or camera input could be stolen by another compromised application and used maliciously, including other connected devices.
- **Information-sharing requirements**: For example, the initial version of Pokémon Go has flaw in an account-creation process that erroneously requested full access to users' Google accounts. .
- **Data localization**: AR devices and applications in particular, can make use of a user's GPS. In addition to (cyber)security, there are legal issues. It is not clear whether any degree of GPS tracking without a warrant is legally dubious, or whether warrant is need only long-term tracking, or there is no problem with collecting such data as long as, for example, the police committed no physical "trespass" onto the person's property, based on United States v. Jones (Wassom, 2016). Pillsbury (2019) suggests that if a user has subscribed to a geo-location sharing application/service, the user could select options for informing other members of their location, notify all automatically (default open), notify only friends, notify specific individuals, request permission to notify when a registered individual comes within a certain range, do not notify (default closed). Similarly, from the marketing perspective, offers/ads could provide real time privacy notice and selections for users.
- Facial recognition software can be used to make false connections with individuals and to take advantage of them, or to identify protesters in authoritarian states thus raising issues of **surveillance**. For example, protestors in Hong Kong in the summer of 2019 used the laser pointers to avoid identification by facial recognition-enabled CCTV cameras or were cutting down facial recognition towers. There are news that the Commission already considers regulation in this area (Khan, 2019).
- There is emerging problem with **deepfakes videos** - doctored videos fabricating apparently real footage of people (see e.g. Hunt, 2019). Deepfakes originated at social media site Reddit in December 2017. [1] Some argue that this danger is not that real since on the one hand, it is not that easy for non-experts to create such a video, while on the other hand it is relatively easy to identify deepfakes videos (Nejedlý, 2019; Schwär, 2019). There already is ongoing political debate on this issue in a Committee of the US Congress (see Kelly, 2019). It is expected that social media platforms will play a key role in tackling this threat (Singh, 2019).
- **Health safety concerns**: AR and VR can distract users from full awareness of their physical surroundings. Thus, there may be risk of injury. For example, Pokémon Go caused distraction and was associated with number of traffic accidents (Ayers et al., 2016). Potentially harmful effects of VR systems to the health of individual users and to society are discussed by Jones (1996).

Source: Pixabay.com

[1] Deepfakes: Fälschungen der nächsten Generation (2019, February 7), https://www.ionos.de/digitalguide/online-marketing/social-media/deepfakes/

User-generated content and new ways of sharing experiences will ensure that issues will arise surrounding **fair use** and **intermediary liability.** The use of AR based apps lead to legal conflicts between AR developers and relevant parties, when depicting a physical space differently, damaging public property (a park), and trespassing and creating nuisances on a private property (Cook, Mariani, Kishnani and Harr, 2019). In several jurisdictions across the world (such as USA and India), use of trademarks 'in commerce' is an essential ingredient to constitute trademark infringement. Thus, the user using a logo in VR may escape liability by claiming 'no commerce' exception under trademark laws. Similar problems arise with the 'fair use' exception under copyright laws of several jurisdictions, wherein there could be an infringement of original works through derivative works on VR platforms (Prajapati, 2018).

It may not be clear where the ownership of **intellectual property (IP) rights** will lie where users have created images or content within the app (MacFarlane, 2017). Even more importantly, VR systems allow users to virtually import otherwise IP protected material into their virtual experiences without obtaining necessary permissions from the owner of such IP.

These issues are intertwined with **real property rights**. For example, does the AR developer need permission from a building owner or a street furniture franchisee to superimpose branding or advertising on their property? (Levi and Furst, 2019).

Moreover, VR users log in from several countries whose IP laws may differ widely from one to another (Prajapati, 2018).

It should be noted that a bill aimed at protecting sensitive locations ("ecologically sensitive," "historically significant," or "dangerous" or on private property) from players of virtual games like "Pokémon Go" was rejected in Illinois (USA) in 2017. It sought to fine developers of location-based video games for not removing virtual stops in the game at a property owner's request (Ruppenthal, 2017, Oosterman, 2016) .

Personal Data protection: There are emerging issues who owns the data, how it should be stored securely, and who has the right to access it. Do individuals have the right to decline being recorded while AR mounted glasses are scanning the surroundings? How developers can identify whose consent they need? Multiple users may use one app, and to the extent that images can be taken, stored and even manipulated, those images may be of third parties who would never be asked for their consent (MacFarlane, 2017).

Targeted advertising - Customisable viewing options will open up new opportunities for companies to be able to leverage personalised data to hyper-target their content, advertising and brands (MacFarlane, 2017). Sponsored content, licensed content, virtual paywalls, in-app purchases and micropayments are significant revenue models for AR and VR apps. As mentioned, regulatory issues may also arise when imposing images over billboards and signs or when receiving advertising revenue generated from other AR ads (Pomfret, n.d.). Furthemore, would advertisers have a claim if AR advertising, perhaps of a competitor, was superimposed on and "replaced" their own real-world advertising or store signage? (Levi and Furst, 2019).

Liability – Negligence Issues: This can be related to Duty of care, its causation and possible damages. What is the 'duty' with respect to augmented reality? (Pomfret, n.d.).

For example, Zhang, Buffington and Toto (2015) ask: „If a player is attacked by a realistic AR character via her head display, and she does not realize that the character is virtual, could she have a claim for assault as a result of her fear or apprehension from the virtual attack?

If the player is injured or injures a non-playing victim as a result of the virtual attack, could she or the non-playing victim have a legal claim against the videogame company or others involved in the manufacture or sale of the game?

If children perform violent acts that mimic their AR gameplay, could victims of those violent acts win a negligence lawsuit?"

A survey among 200 respondents (mostly Executives within an established technology company or Founders/executives of an AR, VR or MR startup) carried out in early 2019, showed, that concerning legal risks while developing ImTe, consumer **privacy and data security** (61%) came out on top. Other top issues for 2019 included **product liability/health and safety issues** (49%), **difficulty in licensing technology and IP** (32%), **potential infringement of third party–owned IP** (30%) and **compliance with platform requirements in publishing content** (30%). Since Dawson (2018) argued that GDPR gives consumers greater control over how their personal data is used and protected, one can assume that higher concern among executives and founders over consumer privacy and data security was an outcome of discussion related to new GDPR rules.

The EU

There is regulation at the EU level targting privacy, cybersecurity and IP rights that applies to AR and VR. This regulation includes GDPR, the cybersecurity strategy and European Agenda on security, part of which resulted in the directive on security networks and information systems (2016/1148), as well as a legal framework covering IPR. The EU regulation on medical devices (2017/745) also includes protection against unauthorised access.

Policy Regulatory Suggestions/Solutions

There are two opposing streams of opinions when discussing whether or not to regulate ImTe.

Moreover, there is not even agreement among experts whether VR could or should be regulated.

For example, Hobson (2016,2) suggests that health and safety concerns that do arise from AR and VR likely would best be governed within the existing framework of tort law, product-liability law and product-safety standards. Similarly argue Cook et al (2019). In their view, before developing new regulations, both businesses and government should thoroughly review current applicable laws and regulations (also for developing industry standards and codes of conduct). In their view, policies that will likely need review and potential reconsideration include property laws, privacy regulations, and copyright and intellectual property rights. Hughes (2017) supports the idea that authorities should increase enforcement or penalties against negative effects coming from ImTe. However, they should not regulate AR app developers under outdated or ill-fitting frameworks, concludes Hughes (2017).

Hein, Jodoin, Rauschnabel and Ivens (2017, 17) also believe that regulation of AR smart glasses can rely on already achieved and implemented regulation, like rules that apply for public CCTV surveillance. However, in their view, policy makers should also account for situations in which sensitivity is needed when weighing different

interests against each other: should there be exemptions to strict regulations about information rights in emergency cases? How are these cases defined? Which property or potential of smart glasses or emergency cases may justify such an exemption? Likewise, rules for daily application need to be freedom-oriented enough that innovation does not become unattractive.

Although collection of contributions by lawyers in Barfield and Blitz (2018, xvi) confirms that the **current legal regulatory framework „will likely be applicable for activities occuring in virtual and augmented reality", nevertheless,, they warn that „as both technologies evolve …..established law may be insufficient...**" Identically, US lawyers Lemley and Volokh (2018, 1138, 1056) believe that **next developments „will require adapting existing doctrines to new circumstances or modifying legal rules to take account of new facts.**...However, it won't necessarily require a fundamental rethinking of legal doctrines. " Similarly, Pomfret (n.d.) advises **to work with lawyers early in the process of searching for regulatory solutions related to ImTe.** Cook *et al* (2019) suggest that businesses and governments can consider launching a **regulatory „sandbox"[2] for AR developers to test ideas before they launch a product in the market**. Within this context, legal firm Pillsbury (2019) suggests for ImTe developers, but also for policy makers, **to develop a comprehensive legal strategy, consistent with one´s business model, to maximize protection of one´s intellectual property, minimize liability for infringement of third party IP, address contractual (e.g., terms of service) and regulatory issues.**

In contrast, Thierer and Camp (2017/2018) **support „permissionless innovation", or the general freedom to innovate without prior constraint (ex ante), as the optimal policy default to maximize the benefits associated with immersive technologies.** The alternative vision—the so-called precautionary principle—would be in their view an inappropriate policy default because it would greatly limit the potential for beneficial applications and uses of these new technologies to emerge rapidly. Thus, in their view, **policymakers should wait to see which concerns or harms emerge and then devise ex post solutions as needed.**

Similarly, Prajapati (2018) suggests that self-regulation by VR companies themselves by adhering to ethical and legally sound policies may be the best solution currently available. However, in case of privacy regulation, he calls for a proactive approach by governments. In case of tortious claims, IR violations and criminal laws, Prajapati (2018) prefers the 'wait-and-see' approach and issues to be resolved on a case by case basis. When defining liabilities, IR holders must state specifically in the contract agreement with VR content creators the ownership and liability arising in case of breach/unfair use of IR or other rights. Identically, corporations and governments must come together to formulate industry specific standards for fair use doctrine.

For example, vendors are already considering software code that could protect against virtual sexual assaults, including "virtual shields, expanded superpowers, or extended personal safe havens to prevent cyber assault" (Harbert, 2017).

In addition to hard law regulation, there are following specific non-legal regulatory suggestions by Banister and Hertel (2018) :

- **Industry standards**: It should be established a sort of AR governing body that would evaluate, debate and then publish standards for developers to follow. Along with this, it should be developed a centralized digital service akin to air traffic control for AR that classifies public, private and commercial spaces as well as establishes public areas as either safe or dangerous for AR use.
- **A comprehensive feedback system:** Communities should feel empowered to voice their concerns.
- **Responsible AR development and investment:** Entrepreneurs and investors need to care about these ethical, but ultimately legal, issues when developing and backing AR products.
- **Guardrails for real-time AR screenshots:** Rather than disallowing real-time AR screenshots entirely, these should be controlled through mechanisms such as geofencing. For example, an establishment such as a nightclub would need to set and publish its own rules which are then enforced by hardware or software.

In conclusion, for time being, the ImTe world is still by and large considered a private space (Oosterman, 2016). However, as technological innovations progress and AR further blurs the line between reality and fantasy, this perception is changing. Especially the launch of the mobile game Pokémon Go revealed public concerns about safety, privacy, cybersecurity, e-commerce, intermediary liability and the intersection between free expression and intellectual property rights. However, **since VR occurs on private, proprietary systems means that the law is unlikely to be used in this area of ImTe,** argue Lemley and Volokh (2018, 1138).

However, Krutz (2018) argues **that the opposite is true**: because it is the process of separation from Genuine Reality that unhinges the operation of the cognitive mind just like poison unhinges the operation of the physical organism, ie the more intense the VR is, the greater the emotional and intelligence complexity that the mind is challenged with to experience. Therefore, **eventually, government will regulate all VR technology and designate its use solely to approved agencies,** concludes Krutz (2018).

Apparently, any discussion on regulation of ImTe must include both lawyers and experts on ImTe technology.

Compiled by SCM

[2] Sandboxes are controlled environments allowing innovators to test products, services, or new business models without having to follow all the standard regulations.