School of Information Technologies

Alessandro Mirani

User Behavior Analysis for Predictive Virtual Reality Applications: An Ethical and Data Security Perspective

Master's Thesis

Aleksei Tepljakov (Research Scientist)
Hayretdin Bahsi (Research Professor)

TALLINN 2019

Declaration of Originality

Declaration: I hereby declare that this thesis, my original investigation and achievement, submitted for the Master's degree at Tallinn University of Technology, has not been submitted for any degree or examination.

Deklareerin, et käesolev diplomitöö, mis on minu iseseisva töö tulemus, on esitatud Tallinna Tehnikaülikooli magistrikraadi taotlemiseks ja selle alusel ei ole varem taotletud akadeemilist kraadi.

Alessandro Mirani

Date: January 3, 2020

Signature: .....

Abstract

Virtual and Augmented reality are emerging, immersive, disruptive technologies that are going to change forever the way people interact. It seems, however, that we are not yet fully ready to go through the consistent changes that this technology imposes. Security, privacy, ethics are all issues that are being discussed this very moment and that are accruing the divide between developers and users. With this study, a survey on users and interviews with various experts from different fields will close the gap in which VR/AR technologies still fall. Starting from a short introduction on this technology and the problematic related to it, a number of solution will be proposed in the attempt of creating a best practice, based on the issues highlighted by the users and with the help of the experts, for collecting and processing personal data in a sustainable way for businesses and in respect of the users' privacy. The aim of this study is also to give a significant input to the ethical debate around the use of these technologies and the effectiveness of the current security awareness techniques; exploring philosophical issues such as responsibility of developers and neutrality of technology will reveal how the cybersecurity perspective can have a say in the present social developments.

The thesis is in English and contains 72 pages of text, 8 chapters, 26 figures, 3 tables.

Nomenclature

AR	Augmented Reality
CAGR	Compound Annual Growth Rate
EDPB	European Data Protection Board
EEG	ElectroEncephaloGram
ENISA	European Union Agency for Cybersecurity
FAR	False Acceptance Rate
FRR	False Rejection Rate
GDPR	General Data Privacy Protection Regulation
IDS	Intrusion Detection System
IVA	Intelligent Virtual Assistant
PII	Personally Identifiable Information
SA	Situation Awareness
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UE4	Unreal Engine 4
USD	United States Dollars
UX	User Experience
VR	Virtual Reality
XR	Extended Reality

Contents

List of Figures

List of Tables

1. Introduction

Virtual Reality is an emerging trend [4, 5]; MarketsandMarkets published a study [4] that shows that the expected CAGR (Compound Annual Growth Rate) of this market is 33.5%, which means that its size will increase up to 44.7 Billion USD by 2024. To give a comparison, in the same time span (2018-2024) smartphone industry has been forecast to grow at a yearly pace of 7,9% [6], while the automotive industry only at a pace of 4,79% [7]. The comparison of these three market shows clearly that virtual reality is gaining popularity at a massive speed. Whether it is due to its usefulness or merely to its novelty, it is indeed expanding aggressively and, to understand the relevance of it, we first have to define what is Virtual/Augmented Reality and why it is so disruptive.

Virtual Reality, or VR, is a technology that "immerses users in a fully digital environment through a headset or surrounding display. This environment can be computer-generated or filmed in 360-degree video" [5]. Augmented Reality, or AR, on the other side is a similar technology that only "presents digital information, objects, or media in the real world through a mobile device or headset. These elements can appear as a flat graphical overlay or can behave as a seemingly real '3D' object" [5]. The distinction here made, should be considered merely lexical, in fact "the convergence of AR and VR is not new from a research perspective" [8] and so, assuming that "the two will likely converge" [8], there is little sense into focusing on the technical difference that still sets these two technologies apart. Moreover, the technical definitions do not exhaustively explain why these technologies will have such a dramatic impact on our lifestyle. What follows is a summary of a few of the many key benefits that this technology has already been able to provide and that have shown a significant impact on the social development:

- **Training for business**: VR/AR technologies allow business owner to perform training and simulation. Hazardous material, life threatening situations and scarce resources are a few elements that made some training scenarios impossible before the advent of virtual reality. The immersive experience guarantees that the trainee is learning by doing, without having to actually be in a environment too risky or too costly to setup [9].
- **Non-physical prototyping**: many companies are already experiencing the benefit of prototyping through VR/AR. Not having to wait for materials and

machinery to building an actual prototype can save weeks to the design process and significantly reduce costs and time that a fully functional product requires [5].

- **Virtual sampling**: VR/AR can help companies reduce the distance with their client by providing them with a sample of the desired product to be tested in real time. Beauty, Healthcare, Fashion industry are already implementing these technologies and are investing even more, counting on the demonstrated potential that will allow them to make the immersive experience applicable to a wider array of products (not just clothes) [10].

- **Digital learning**: VR/AR in parallel with the development of the entertainment and gaming industry is expanding the possibility of the digital learning industry. more interactive and immersive experience that can occur in digital classes can lead to a border-less, more engaging, education [10].

These are but a handful of applications that already are being used and yet show massive growth potential. However this disruptive, eruptive technological development brings new challenges on the security and ethical side. For example, reports of sexual harassment in Virtual Reality [11] have already been divulged to the public and more concerns over the safety of these devices are being fomented, due to existing or novel question over the reliability of these systems and the real data processors behind them.

Umberto Galimberti, philosopher and sociologist, said that in modern times "technology is not a means at the disposition of man but the environment in which man undergoes modifications" thus "the question is no longer *what can we do with technology?* but *what will technology do to us?*" [12]. With VR/AR, ironically, we truly enter an environment in which we undergo modifications due to the engaging experience. Bullying, physical harm, panic and other painful circumstances can be lived through the VR/AR experience [13, 14, 15], thus making the threat these technologies pose very much real and the philosopher's question even more scathing: what can VR/AR do to us?

The opportunities offered by these novelties are as exciting as the challenges posed by the innate risk of technological development. This dissertation evaluates matters such as cybersecurity, data privacy and ethics in VR/AR environments to keep the advancing of this world-shaping changes on the right track. In the next section, the

research question and the posed goals of this study will be presented.

1.1. Research Question, Goals and novelty

The main goal of this research is to investigate:

1. Whether a person can be positively and uniquely identified based on recorded motion and single-channel EEG[1] data?
2. Assuming this data is sensitive, how to securely collect, transmit and store it?
3. Explore data ethics considerations in this research: how can the modern ethical frameworks improve?

The goal of these question is to provide a best-practice model that compounds data privacy, cybersecurity and ethical standards up to date. The novelty of the work consists into considering, alongside privacy and ethics, the physical and virtual security aspect and making a of case scenario through the use of a physical laboratory in which was tested the application of the mentioned technologies for research purposes. Both the goal and the research design have been formulated on the model of previous research in the same field, such as research on ethical or data privacy issues [17, 15, 18, 19, 20, 21], but with different applications; in particular, in this study the focus was posed on data collection for predictive analysis that respects legal and ethical standards. No ethical or legal framework however can be considered complete, in the author's opinion, if not integrated with security notions, as the "cybersecurity issue" too is an emerging trend [22].

Stepanova et al. [23] have designed a research method for a best practice in UX design in VR Space Training programs, making use of the same methodology: they initially collected literature, corroborated the findings and explored new angles through personal interviews and then designed a series of qualitative models to propose a solution to the most highlighted problems. A similar model will be presented in the methodology section, explaining step by step how this research developed.

The limitation of this dissertation is that it does not cover all the technologies that can be implemented in VR/AR applications, the focus was posed on the more widespread technologies in the market. This is due to the fact that the technology, while certainly showing potential, has still a low adoption rate [24]. No study has

[1] Electroencephalography is a method to record the electric signals emitted by the brain [16]

been made on VR/AR devices, specifically, with a cybersecurity approach that would include the opinions from users and developers. For this reason, a questionnaire survey and a pool of interviews, highlighting the most common security problems in the user experience with VR/AR technologies, was designed to complete this study.

The main cyber attack vectors considered for the lab environment were spoofing and impersonation, meaning the theft of data on the transmission channel and the false representation of an individual in a cyber environment. These attack vectors were considered the most likely to occur based on observation made on the laboratory facility. Any other vector that would have included attacking a third party service provider was not considered, as the necessary information to conduct a meaningful analysis (such as the cybersecurity structures) is not publicly available.

The key assumptions are that the technologies with which was impossible to perform experimentation (such as headsets from other vendors or newer models of the same headset) in real life scenarios share similar feature (in their hardware or in their application) such that they can be assumed equivalent when disserting about cybersecurity, privacy and ethical issues related to the VR/AR landscape.

2. Literature review

For the purpose of this dissertation, firstly was evaluated which technologies were most common and widespread among the market. in order to do that, the conclusions were drawn based on the Valve Corporation's Steam hardware survey [25]. As of 2019, Steam counted 1 Billion accounts (roughly), for a total of 90 Million active users worldwide[26, 27]. The store offers more than just entertainment software (professional software and training software are also part of the catalogue) and it offers support to all VR/AR devices compatible with the software sold on the marketplace; given the size and the variety of the users as well as the number and variety of software included in the Steam catalogue, it would be appropriate to estimate the spread of hardware based on the data collected by Valve.

According to Valve's survey, HTC Vive and Oculus Rift are the most widespread VR devices, amounting to almost 90% of the total number of devices owned by users worldwide. For this reason, the focus was posed on these two devices in particular during the literature gathering phase, by searching for these two devices the keywords mentioned in methodology. The aim of this literature review was to answer the first research question: can a user be identified through the data collected through these devices?

What emerged from literature is that it is indeed possible to identify people based on data collected through VR devices; in the next sections will follow an overview of the mentioned technologies and the way they collect personally identifiable data.

2.1. Personal data VR/AR technologies

Oculus Rift and HTC Vive use a similar system to track motions; both these hardware implement a data-flow system that can be described as shown below in figure 1: blue arrows represent movement data stream, red arrows represent the path of mixed data (video, audio, motion).

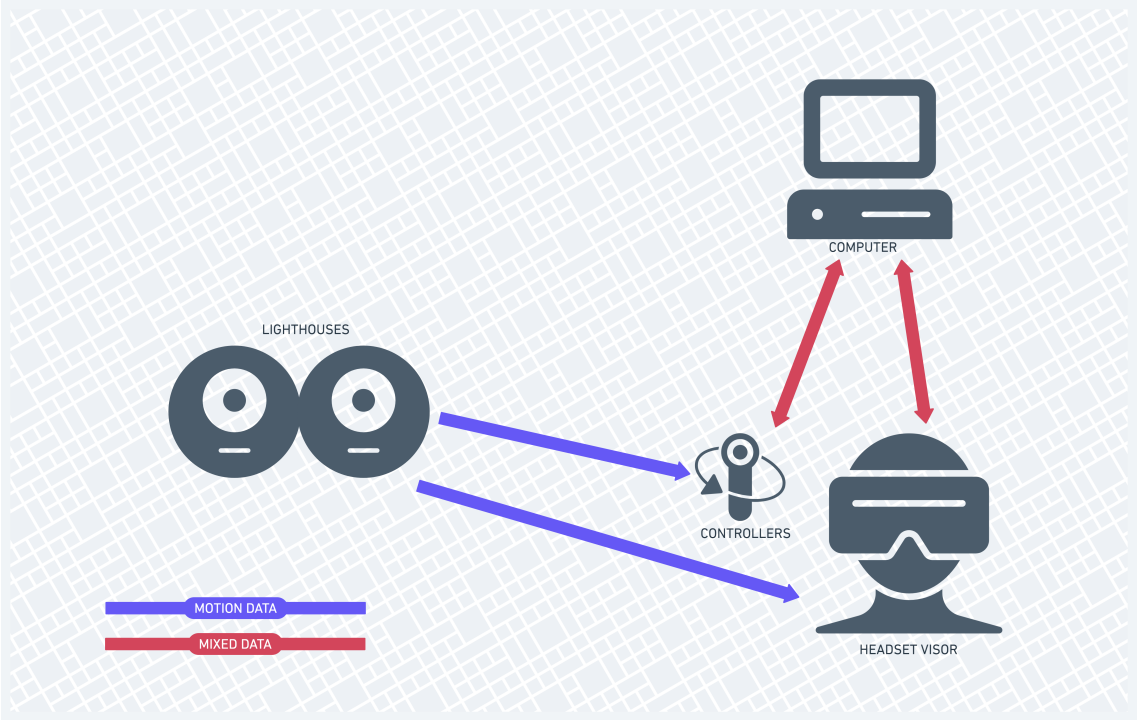

Figure 1. A generic model of data flow in VR/AR devices

The controllers and the headset movements are tracked through sensors or lighthouses (HTC Base Station and Oculus Sensor), located at a suitable distance; for HTC it can be more than a few meters, while Oculus Rift sensors track optimally between 1.8-2.5 meters. However, both controller and headset send some different data (like controller inputs) to the computer that processes altogether depending on the application running. Although the two hardware differ in terms of aesthetics and technical design, they are very similar in the way they work and allow movement data to be captured. The same can be said for the newer models, HTC Vive Pro and Oculus Rift S, which offer a different user experience but rely on the same structure shown. In these structures, we can see how all the three pieces of hardware contribute to transmit data independently and interdependently at the same time. The lighthouses are autonomous and yet need the controller and headset to generate meaningful data; the controller and headset do transmit data to the computer but the data would be in most cases incomplete if it was not computed with the information coming from the lighthouses.

Coming back to the matter of whether the data collected through such devices should be considered personal or not, more sources [28, 20], clearly demonstrate that it is indeed possible to identify users through VR-device-collected data. In particular,

Pfeuffer (et al.) [28] have performed a study in 2019 that reveals that motion tracking in VR [28]can lead to personal identification through:

- Throw pattern
- Head-tilt[2]
- Gaze tracking
- Hand movement

They also state that their result have proven that with these devices they managed to reach "soft biometric accuracy" [28] (strong biometric accuracy generally considered above 90% [32]). The results were mixed with an accuracy sliding between 30 and 60%, depending on the size of the test groups (the higher values of accuracy were registered with smaller groups of test subjects). To offer a comparison terms, in 2018 Google [32] deemed "low accuracy biometric" every implementation that showed a FAR[3] (the rate at which false results are accepted) higher than 7%. In this sense we could say that, at least for android application, the findings of Pfeuffer, if implemented in an AR applications for Android, could achieve the goal of biometric identification and at the same time be very prone to security issues, as they allow personal identification, but are very much prone to error (not up to Android standards).

On the other side, others like Banerjee (et al.) [20] used a task-driven approach and obtained much more accurate results. Task driven means that they required their users to perform an action (in most cases just throwing an object such as a ball) in a virtual environment, then registered the movement pattern. On a sample that counted 135 test subjects they reached 92.85% accuracy.

[2]Head tilt refers to the unique way a person moves his/her own head; the expression is widespread in literature (Majed et al.[29]). Head tilting is in fact one of the standard inputs method, as it defines (in most applications) where the gaze of the immersed user focuses, but it also can have more applications to the point it can substitute other controller inputs; for example, Yan et al. have perfected this concept design to the point where they made possible to perform "gesture movement" and "drawing shapes" with the use of head in VR environments[30]). Head-tilt here on after (and in literature in general) does not refer exclusively to the voluntary movement of the head, but also to the "unintentional motion"[31, 30] (inertial movement, not necessarily intended or planned by the users)

[3]False Acceptance Rate, meaning the rate at which an element is mistakenly considered valid, is one of the key biometric assessment statistics, along with False Rejection Rate (FRR); we keep into account FAR because it is particularly relevant for what concerns spoofing and impersonation attack vectors, which are of interest for the subject of this study. For the case of FAR, the higher the rate the more prone the technology is to error, thus leading to lower security by design [32]

Android, operating system used on billions of mobile devices worldwide, implements biometric recognition systems on its devices that have a 93% accuracy rate [33, 32, 6], which mostly are fingerprints sensor [34] (a broader and more established biometric system) and only in the recent years to face recognition[4], which has been implemented for more than three years now. We can thus say that Banerjee has found an accurate enough system to be up to standards for being implemented on billion of devices worldwide.

Additional literature review on more diverse VR technologies also has shown the following findings:

- Armstrong (et al.) achieved a 97% accuracy rate on brainwave pattern biometric analysis [17]. Although brainwave data is not used in commercial VR headsets, in " Re:creation VR First" [36] lab, for example, the combined analysis of brainwaves and other data collected through VR is being explored; knowing in advance that EEG can indeed be used to uniquely identify someone, as with data from other VR peripherals, can make us conclude that the combined analysis of EEG plus another of the most common data (like the ones in the previous list[5]) can certainly lead to personal identification.
- Zaho [37, 38] found out that motion tracking can be used to predict relationship between movement pattern and health conditions (the research focused analysis on posture of care-taker during surgical operation to establish how it is related to backbone problems). The data collected and observed has been thus classified as sensible and relevant for medical purposes. For the purpose of our research, is interesting to note that we will keep the same data and that it can be used for the same purpose; the researcher in this case solved the privacy issue through a registration process that required candidates to sign an agreement, however they did not elaborate more than that on how they stored and collected data.
- Alam [9] created a AR/VR IoT system to perform maintenance tasks. They handled security on the network level through symmetrical encryption (pre-shared key). They suggest the use of CCAF (cloud computing adoption framework) multi-layer security which requires: firewall, identity management, and encryption.

[4]Trusted Face, was one of the first services available for Android and it was developed around 2015 [33] and in 2017 was fully implemented in compatible Apple devices [35]

[5]Throw pattern, head-tilt, gaze tracking, hand movement

- Qureshi [37] solves the issue of privacy preserving in video surveillance by converting videos in object streams. Color coded objects allow: selective rendering, improved analytic and "object-centric decomposition" [37], that improves the ability of the operators to focus attention on the relevant details while concealing the identity of the recorded subjects.

- Roesner [39] asserts that AR technologies that make use of face recognition can be used for lie detection and other physical deception attempts. In fact the most common sensor that are on the market can be used to authenticate with biometric and behavioral characteristics. Furthermore, AR sensors can be used to implement distributed trust systems, where a person's identity is validated by bystanders rather than one specific users.

- Sekhavat [40] studied the privacy issue related to the us of a Try-On Cloth application that used AR. He solved the issue by splitting the data collected between server and client side. This way, both server and client are unable to single-handedly to gain meaningful information without the counterpart's data. This technique was adopted in conjunction with a "secure computing technique to make sure the computations of the model modification functions are performed securely on the server" [40] and Fully Homomorphic Encryption (FHE) algorithm to remotely perform computation on semi-honest cloud servers.

- Fung [41] studies the privacy problem arising from releasing person-specific data. The solution proposed is "to mask unnecessarily specific information into a less specific but semantically consistent version" without incurring in consistent loss of cluster quality. The research focused on 3 key masking operations: generalization, suppression, and discretization. The research crew managed to create a "anonymization algorithm called top-down refinement (TDR) that can perform all three types of masking operations" [41] with successful results on most of their data-sets.

- Xu Ma and Tian [42] studied the privacy issue that arise in the process of data publishing. After reviewing a model that resumes that stages that data goes through (from owner to recipient) they make a study on: data-linkage attack models. Taken into account the background knowledge of the attacker and the information metrics involved, they assert that k-anonymity methods mixed with other elementary anonymity techniques is a sufficient combination to effectively anonymize the data in the process.

Based on this research, it can be concluded that VR/AR technologies do collect personal data that can be used in different ways not only to identify a person based not only on visible traits but also on non-visible, such as heartbeat. There are different ways to anonymize data but there is not a best practice yet in place and it also must be considered that the literature so far reviewed was international thus not all the authors were subject to the GDPR standards. What is also interesting to notice is that some research over cross-examined data has revealed a sort of "transitivity" in the properties of PII, so that if some information is PII per se, it will preserve this property when cross-examined with other data. Thus, from this section on, whenever will be made reference to PII data collected through multiple components of VR/AR devices, it should be assumed that at least one of those components is collecting PII.

2.2. Ethical issues that emerged through literature research

For this study we take into examination the ethical questions concerning the democratization of VR/AR technologies. In order to define which ethical issues will be examined, we must first define what ethics are.

"Every action and pursuit is thought to aim to some good" in Aristotelis', father of ethical philosophy, thinking [43]; thus "shall we not like archers[...]be more likely to hit upon what is right?" [43]. In other words: assuming all our actions aim to a superior good, we should logically be seeking to achieve that rather than anything else. "If so, we must try,[...]to determine what it is [the good]" [43]. In the study of what is the "good course of action" it is important to question the definition of good and bad. Thus the purpose of literature review was to highlight the issues that caused controversy on the "good" or "bad" use of technologies that at least shared relevant features with VR/AR devices, so to have a base for the questioning of the ethical use of VR/AR, which will be done in the following sections.

As demonstrated before, VR/AR devices can be used to uniquely identify a person [44, 40, 20]. But data security and privacy are only two of the issues that arose in recent year from the development and mass spread of these technologies. In this section follows a review of some of the more severe and invasive issues that have drawn the public attention and that are assumed (in some cases) to be an essential part of the VR experience.

Post traumatic stress disorder can be caused by experienced by a compelling experience that does not offer a relief [13], also children's memory is more sensitive to the content assimilated through virtual reality more than through Television broadcast [13]. VR is immersive, so its consequences: motion sickness, disconnection from real world (fire alarm, environment threats), virtual harm (bullying intentional scare) [15], also:

1. Chung et al. have analyzed PII collected by IVA systems (Intelligent Voice Assistant) [45]. On the basis that the information collected by these devices can be used to "construct voice artifacts that could be used to impersonate these individuals" [45], they analyzed the social implications. In particular they weighted the benefits that this technology offers against the possible issues that it poses, for example "[b]ecause speech recognition is not a perfect science, it is possible to eavesdrop on private conversations unintentionally", concluding that "and privacy threats of these IVAs have not received enough attention" [45]. The risks behind the speech recognition technology are shared by all the devices that implement speech recognition features[6]), as they allow the users to use a "trigger word" or "wake word" [46] to be turned on. For this reason, in the Alexa case the microphone needs to constantly record in order to correctly process the order and VR headsets can share the same feature[7].

2. Brad Smith (Microsoft Chief Legal Officer) attributes to the Cambridge Analytica scandal a part of the mistrust that today's consumer have in big companies [47]. Facebook CEO Mark Zuckerberg has admitted to be responsible for a breach of trust towards its clients [48], however recent studies show that the customers are more concerned about their privacy than before after the facts of Cambridge Analytica [49].

3. On the issue of personal data misuse also, various state-level issues were analyzed, the most controversial of which seemed to be the China's Social Credit System [50], a face-recognition based system that assign scores to citizen based on their behavior in public places. It is renown that Chinese government has implemented this Social Credit System, in works since 2014 and that is

[6]IBM has developed a voice interaction tool that works both on HTC Vive and Oculus Rift, allowing virtually any developer to integrate "advanced interactive speech systems for virtual reality" in their programs

[7]Again IBM provides the full documentation to make the aforementioned features work also with wake word, specifically to reproduce the functionalities of similar services offered by Amazon and others[46]

sought to be officially implemented by 2020 [51, 50, 52]. The debate surrounding this system seems to highlight a high degree of controversy; some people argue that this social control causes is source of more drawbacks than advantages, other asserted that is an extreme solution to a "problem the ruling party itself has created" [52], thus questioning the proportionality of such control to simply deter criminal behavior. These problematic were taken into account due to the fact that the misuse of data performed at state level is an ethical issues that applies to all technologies that collect PII; given the demonstration offered in the previous section, on how much data VR/AR devices are capable of collecting, is very important to pose these questions while these technologies are being developed.

4. Again on bigger scale a less political problem, that is still worth investigating is "the problem of many hands" [53], or the distribution of the responsibility across many actors. Another problem concerning the collection of PII is that if (when) leaked, is hard to build a reliable chain of responsibility, as the concept itself of responsibility tends to blur when many actors are involved in a single process and most of them are "simply a functionary with no final responsibility" [12].

5. Virtual applications have shown the potential of inducing addictions [54]. Virtual reality offers a degree of immersion that goes even further normal application thus having a greater potential to cause these issues. This interesting issue has been later abandoned, in following stages of my research, as the results from both literature and other sources were too fuzzy and unreliable. Also such issues are being now explored from a constructive perspective, at least for what concerns virtual reality, as it has been demonstrated through research that VR/AR devices can help cure addiction caused by gambling, tobacco and other causes [55].

These were the main thematic explored during the ethical investigation. The literature review over ethical issues has certainly arose more problems than solutions, as it is to be expected from an ethical debate.

In the next section will be highlighted which were the most notable gaps found in the so far reviewed material.

2.3. The gap in the literature

As can be seen in the previous section, most of the literature either focuses on how to collect personal data through VR/AR devices or how to anonymize it. There is no detailed focus on the problem of data security, there are only a few cases in which a data security framework is described [38, 37, 40]; the information is usually incomplete and does not allow to devise a precise guideline to follow in order to create a cyber-secure environment for VR/AR experience.

The same goes for the methods to securely store and transmit data with VR technologies. For what concerns the ethical issues, little study has been made about the deeper risks (as the ones highlighted by the authors quoted in the previous chapter [45, 48, 52, 12, 54]) of connecting the world through such an immersive experience and in the few contexts in which it has been made, there is no mention of the data security problem [15, 21, 56, 11].

In general, the literature so far produced seems to consider privacy, security, user experience and technical development as separate containers. At least for what concerns modern cybersecurity research, a shift towards the "multidisciplinary approach" [1, 19, 57] has granted better results in terms of Situation Awareness and control; a practice that has not been adopted yet regarding the specific issues of VR/AR, probably due to the novelty and the rapid changes that are in this sector.

For the same reasons, is hard to find standards and guidelines regarding safety, security, ethics in this sector; that most of the sources reviewed for this study did not reference any previous source for the security models implemented, demonstrating that this field of research has just started to develop. This consideration is corroborated by the lack of a strong answer over the pending ethical issues that have been explored and that pose a challenge to modern research with VR devices due to or prescinding from the issue of cybersecurity issue.

Also, the ethical literature so far produced offers many points of view and demonstrate the controversy and complexity of the present debates, but, despite this, it never offers an ethical judgment system, on the base of which would be possible to draw a conclusion.

In the next section, follows the description of the methodology that was considered

best fit to answer the research questions presented.

3. Methodology

The literature has been collected through a web search run on different keywords sets, such as: privacy preserving, data mining, data publication, AR device, XR device, VR device, attack vector, best practice, cybersecurity.

Of these, the combination that produced the most results are:

- privacy preserving data mining,
- privacy preserving data publication,
- personal identification VR device,
- attack vector VR device.

the websites used to gather primary sources for the research were IEEE Xplorer [58], Google Scholar [59], Researchgate [60] and ScienceDirect [61]. Secondary sources sources like web pages and online articles have been taken from pages found through normal search engine, provided that they satisfied authoritaritiveness standards, following these guidelines [62]:

1. Prefer acknowledged authorities to self-proclaimed ones.
2. Prefer an authority working within his or her field of expertise to one who is reporting conclusions about another subject.
3. Prefer first-hand accounts over those from sources who were separated by time or space from the events reported.
4. Prefer unbiased and disinterested sources over those who can reasonably be suspected of having a motive for influencing the way others see the subject under investigation.
5. Prefer public records to private documents in questionable cases.
6. Prefer accounts that are specific and complete to those that are vague and evasive.

7. Prefer evidence that is credible on its own terms to that which is internally inconsistent or demonstrably false.
8. In general, prefer a recently published report to an older one.
9. In general, prefer works by standard publishers to those of unknown or "vanity" presses.
10. In general, prefer authors who themselves follow [standard] report-writing conventions.
11. When possible, prefer an authority known to your audience to one they have never heard of .

A source was thus considered authoritative provided that it satisfied 7 of the 11 quoted conditions (more than 60%).

A few examples of subject categories are: acknowledged news publishing companies' articles, industry leaders' reports, official government pages' documentation. These sources were used to conduct a preliminary research (a literature review) on the research questions. They allowed to shed light on whether or not the question posed was relevant and had been already answered. The research questions demonstrated relevance, although they had not found a reliable and capillary answer to the issues analyzed. To make a meaningful contribution to the existing literature, the analysis needed to make emerge how these issues are widespread among industry developers and users. Two separate methods were used to assess this phenomenon:

1. Semi-structured interviews with industry developers:

   The interview was conducted on the basis of the following questions:

   (a) Data transmission and collection
      i. Did you encounter any data privacy issue in your work?
      ii. How did you solve it?
      iii. Did you encounter any obstacle in implementing your solution?
      iv. What was the lesson you learned concerning data transmission and collection?
   (b) Physical environment structure

i. Did you ever face a security breach/attack to your environment?
ii. How did you face it?
iii. My lab works like this: [...]. Based on your expertise, what vulnerability or inefficiency can be improved?

(c) Ethics

i. VR will enable new types of crime, such as stealing goods and attacking physical person or causing physical/psychological harm through virtual experience, have you ever faced such problems?
ii. If yes how did you approach them?
iii. If no have you ever thought your technology would be prone to such dangers?
iv. Who would you consider responsible for such issues?
v. How would you solve them?

2. Questionnaire for users (all close questions except the ones marked with star):

(a) Category awareness/usage

i. How familiar are you with Virtual/Augmented Reality products?
ii. How would you describe your overall opinion of this product category?
iii. When you think of this product category, what comes to mind first?*
iv. Where did you go to find out information about the systems?
v. What do you usually do with VR?
vi. What do you see as the benefits of virtual reality?

(b) Concerns

i. When you were making use of VR devices, did you have any concerns regarding your safety or health?
ii. Why/why not?*
iii. Would your opinion on your device change if you knew it exposes you to health issues?
iv. Did you worry about privacy when you were using your device?
v. Would your opinion on your device change if you knew it exposes your personal information?
vi. Did you worry about security when you were using your device?
vii. Would your opinion on your device change if you knew it exposes you to cyber-attacks?

viii. Do you still have these concerns?

(c) Data Collection

i. Do you think your virtual reality system collect information about you?

ii. What do you think it collects?

iii. How do you think this information is used?

iv. Are you concerned by this?

v. Would you say you feel differently about data that gets collected by our other devices?

(d) Recommendations

i. Would you recommend VR to people close to you?

ii. If all the concerns you expressed in the previous sections were addressed how much would your interest/experience in VR technologies improve?

Both questionnaire and semi structured interview have been devised on the basis of similar studies conducted with the same strategy [15]. On the basis of the questionnaire results and the literature review, a best practice for setting up a Virtual Reality environment that collects ethically and securely user data was devised. The feasibility of such lab has been then corroborated through real life implementation, interviews with experts and literature review [2, 63]. Finally, a recommendation for future work will be given, based on the limitations and key assumptions of this work.

Limitations are that:

- The technologies reviewed are the most popular up to November 2019 [25], thus the work cannot cover issues arising with later developed technologies
- Although the literature has been collected through worldwide research, the industry developers and users have been surveyed across European countries, thus validating only for this particular geography the ethical concerns highlighted and the conclusions drawn
- The physical solutions suggested in the thesis are only valid for a small-medium size company (10 to 50 employees) as they have been formulated and validated based on the knowhow of similar businesses

Key assumptions are that:

- VR and AR devices with similar properties can share similar problems/solutions
- Due to the growth in size and profit of the VR/AR market, cybercrime in the same market will be a matter of interest in the future
- That the regulation in place will not have radical changes in the future that invalidate the purpose of research in the matters of privacy and security

On these considerations, suggestions on how to embetter the work developed in this study will also be given.

4. Results from the questionnaire

The same literature, from which the questioning model was drawn [15], showed that for a better result the selected candidate needed at least a basic experience with VR/AR technologies. Thus, the questionnaire was sent over selected groups of people. Given the nature of the questions, the ideal pool of candidate to obtain meaningful result would have contained people of any gender, race or age with the only discriminant of at least one basic experience with VR/AR. In order to achieve that, the groups of people were selected mainly through social media and academic contacts that had profiles correspondent to the desired one. Also, a disclaimer was put in the presentation of the form's link as well as in the introduction to the questionnaire, referring to the fact that it was aimed to people with at least basic experience with VR/AR devices. Furthermore, the first question (self-assessment over the product knowledge) was designed so that it could serve as an additional benchmark for the quality of the candidates pool. It was then decided to filter out the replies of the candidates that did not consider to have any familiarity with the product. Of the 165 candidates only 5% of them described themselves as not at all familiar with the technology.

As first assessment of the quality of the replies, the first statistical tool used was the linear regression between two questions: "How would you describe your overall opinion on this product category?" and "Would you recommend VR/AR devices to people close to you?". It would have been considered a bad indicator seeing a correlation negative or neutral between these two questions, as it is intuitively expected that a person with a higher opinion of the product would recommend the same product more strongly.

As a matter of fact, it has been possible to observe a good positive correlation: Multiple R[8] value was 0.54 with a significance of F close to 0 $(4.1E^{-13})$[9], which indicates a very high reliability of the obtained Multiple R value. These values

[8]Multiple R is the main correlation value, it fluctuates between -1 and +1, where -1 is very strong negative correlation, +1 is very strong positive correlation and 0 is no correlation at all

[9]Significance of F indicates the reliability of the correlation value, the lower the significance of F the more reliable is the correlation

together suggest that a trend is indeed present between the two questions and with a good reliability. On the basis of these three considerations:

- that the pool was carefully selected and the self-assessment showed a very low number of inadequate profiles thus confirming the validity of the method
- that the questionnaire was designed to discourage random questions
- that the regression between the first and last questions shows a logical and reliable trend thus confirming the effectiveness of the choice of design

The obtained results are reliable and it is possible to make relevant assumptions on the following bases.

Given the close nature of the semi-entirety of the questionnaire[10] we decided to give more weight to quantitative analytical tools. What follows in the next section is a graphic representation of the obtained answers with comparison with the literature used as methodology base.

4.1. General product perception

As shown in figure 2, most of people did not mention online channels at all as a source of information, in accordance with the studies developed so far; however friends, family, school and university seem to play a bigger role than anticipated by literature as they were both mentioned as a source of information by 37% of the users, while in literature review only 1 in 10 candidates quoted school as a source, and only 2 in 10 quoted friends and family. It must be noted that these differences might also be due to regional reasons, as the main audience for my questionnaire was Europe, while the literature reviewed focused on an American audience.

[10]Of a total of 20 questions only 2 (10%) had an open nature and required only a short answer (the acceptance threshold was set to a minimum of 8 words)

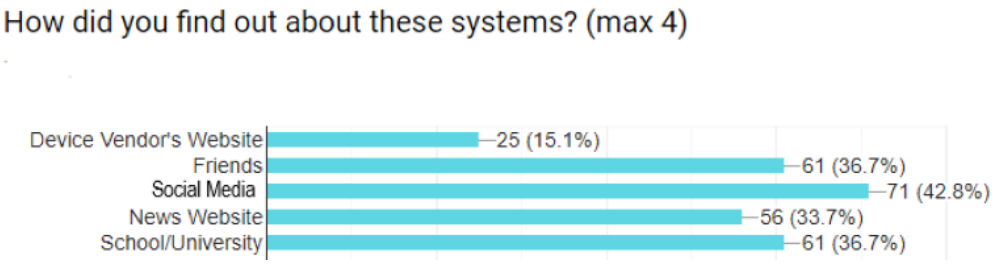

Figure 2. The most common channels indicated by users to get to know about VR

As an ice breaker, the users were also asked to describe what first comes to their mind when speaking about VR. This question was not intended to serve any specific purpose, if not understanding generally what bias and what perception do people have around VR. A summary of this reply can be seen in the following graph:

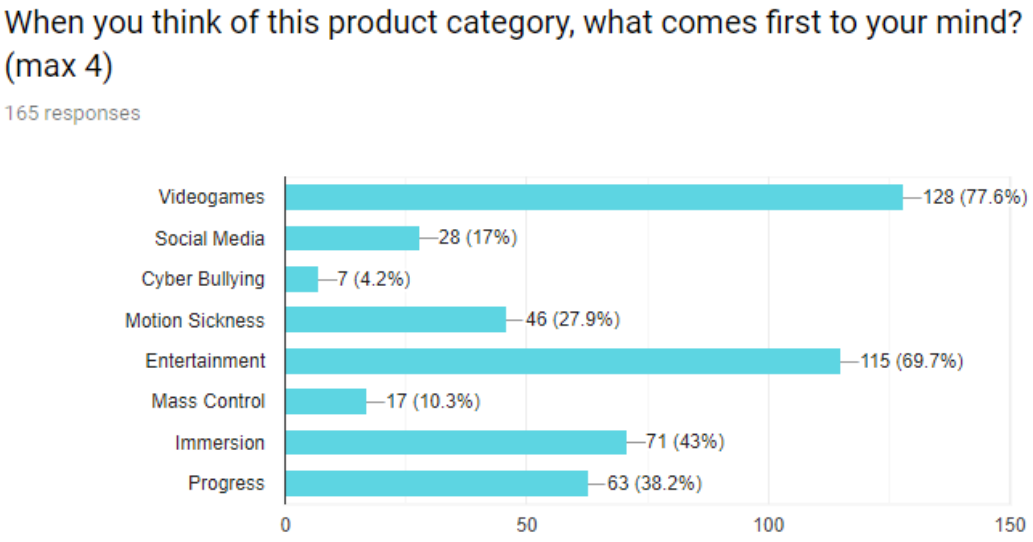

Figure 3. A summary of what comes first to people's mind when talking about VR

As figure 3 shows, there is still a strong bias around VR as a media for videogames, however this connection is not exclusive as 98% of the users that mentioned videogames mentioned something else, for example 21.7% of the users that mentioned videogames also mentioned social media. On the other side 27.9% of users also mentioned motion sickness, which indicates that this problem is in many users mind when approaching this technology, however, more on this will follow in the upcoming section.

Moving on in the questionnaire, the users were asked more in depth questions over their experience. As figure 4 shows, almost 68% of the candidates gave little to no relevance to safety or health in their VR experience, going against the trend seen in literature where the safety concerns were raised more on the user side than the developer side; could this have been some sort of population bias? No data is available to assert this with certainty but it seems this is an inverted trend when compared with the literature reviewed, thus might indicate that smaller populations are self selective even when all the due care is taken in having a mixed pool of candidates. The data is even more against the reviewed trend if we consider that in the following question almost 60% of the candidates replied that they lost any concern after becoming familiar with the VR technology (figure 3).

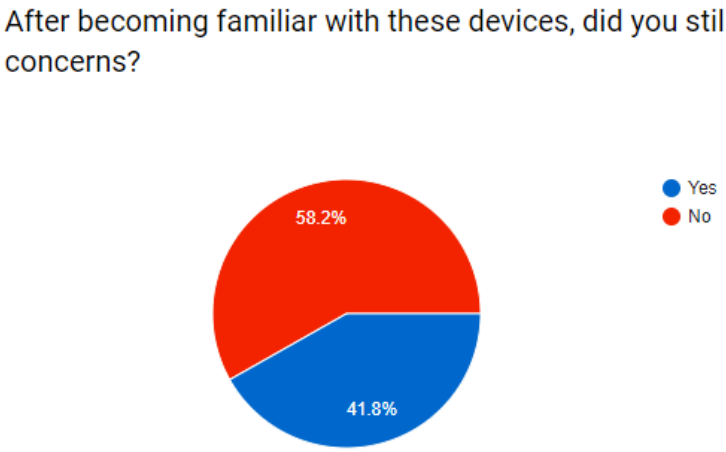

Figure 4. Change of opinion after experience with VR/AR devices

In the following section, where users were asked why they felt concerned (or not) in open form; after reviewing one by one all the answers four main categories of answers were derived that can describe the users' reactions as follows:

1. **I was concerned because of motion sickness (note that a few, after expressing this concerned pointed out that they actually did not suffer from it yet), excessive immersiveness (that leads to disconnection or "bumping" in physical environment), privacy/cybersecurity issues:** 28.5% of users, said that their concerns originated due to technical aspects of their devices such as motion sickness and security/privacy features.

"Bumping" in physical space, disconnection, fear for disconnection and addictiveness were also expressed as concerns. Someone even mentioned strong negative experience as a cause (physical harm, strong motion sickness). Some others remarked that their concern was not coming from a real-life experience but from what they "heard about VR".

2. **I was concerned because I was not familiar with the technology, long term effects or I felt the vendors was not informing me properly in general:** 9.5% of users indicated that their concerned originated from scarcity of information over health implications and data usage. Many made comments referring to the long-term perspective in particular, pointing out how, even with all the resources available, it would be impossible at this time to fully understand long-term implications of using this technology.

3. **I was not familiar with the technology but I was not concerned about the risks:** 15.5% of users expressed that they were not concerned simply due to the fact that they did not know the technology. Similar to the previous category, these users expressed a lack of information, however their overall sentiment over this condition was completely neutral.

4. **I was not concerned because, although I knew the risks, I either ignored them or realized I would overcome them easily:** more than one in three usesrs (36.9%) had a positive experience at the point where they felt in control of the risks encountered. In this category fall people that have expressed particular trust in the manufacturer, in the legal standards in general, or that simply feel in control of the technology and its consequences. Some others made it a "survival of the fittest" question, implying that since is a mandatory progress it is better to use it, but always with positive remarks (such as smile emoticons or soft words).

it is worthy to note also that, combining category 2 and 3 net of their sentiment, we can say that 1 in 4 users (25.5%) is victim of information asymmetry in the VR/AR landscape. This data should be even more concerning considering that is possible to assume that people with a positive sentiment (category 4), felt such not due to a compelling good experience but due to simple lack of information over the possible dangers, as more than a few replied: "what's the worst that can happen?"

4.2. Data collection awareness

Moving on, the users were asked more in depth about data to assess their awareness and to explore their sentiment over data security. It must be noted that these question generated a little bias, as the order in which was put forced users to answer on the data they thought could be collected through VR/AR regardless of whether they actually thought it would be collected in the first place. With awareness of this fact, the intention was in fact to assess what was the bias and the perception around this technology rather than assess the precise knowledge of the users. In the end, it seemed a good choice as almost 40% of the users replied that they did not think that any data was collected through VR/AR devices.

This data reinforce the hypothesis expressed before, as if we sum up the users that declared themselves uninformed we reach roughly 25% of total users, so even if we assume that all the people that ignored that personal data is collected through VR/AR devices are coming from group 2 and 3 of the previous section, we still have a rough 15% of users that are not informed properly and do not realize the data collection happening with VR/AR technologies. Again, the unsolved question would be: how many of them are part of the category that had a positive experience?

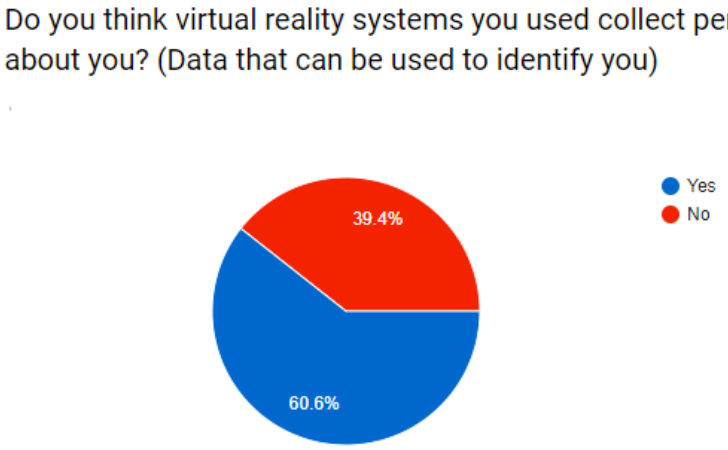

Figure 5. Data collection awareness with VR/AR devices

Assessing only the perception of the more aware people would have resulted in a loss of almost half of the pool's opinion over the information collected through VR/AR devices, so it must be considered that the next answered is extremely biased and in most cases it was a guess from the users. Given the fact that the answer allowed

open replies too, here again the prevalent categories of answers that emerged will be summarized:

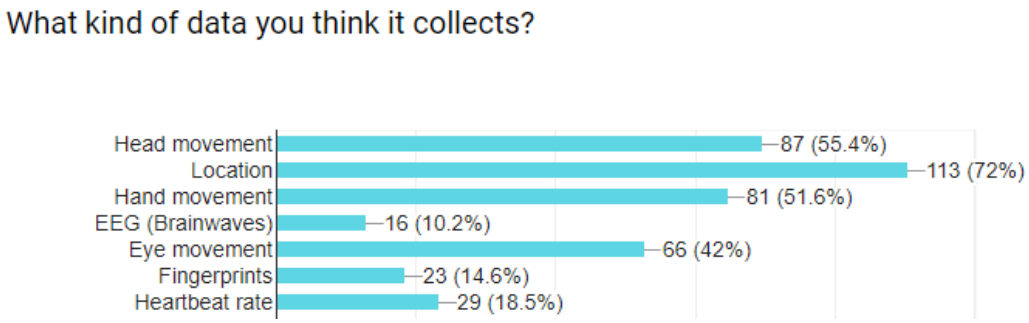

Figure 6. Summary of the question: "What kind of data you think it (VR/AR device) collects?"

As it can be seen, vast majority of the users assume that their location is collected, a data that is quite interesting to analyze as most of VR devices do not collect location directly as most of them do not even use a GPS. Only phones can be considered VR/AR devices that collect location, however, as Bain&Company demonstrated with a report in 2018, VR/AR technologies have seen an adoption rate as low as 13% on mobile devices; these numbers are too low to justify by themselves the fact that location is the most assumed data to be collected. Furthermore, in the same year fingerprint sensors on mobile device is practically becoming a standard as its adoption rate was forecast for as high as 71% [34]. Even without assessing how many of devices with fingerprint sensor (or without) are capable of run VR/AR application, the disproportion between these two features adoption is evident and still of all the users surveyed only 14.6% replied that also fingerprints are collected as well.

We could assume that that 14.6% of people that ticked the "fingerprint" box is wholly composed of that 13% of mobile users that use their phone as AR device; in fact, 11.5% of all the questionnaire candidates ticked both fingerprints and location boxes, so the assumption could be even backed up by this data. However, if we subtract all the users that have ticked both fingerprints and location from the total users that have replied location, we still are left with 61.5% of users assuming that location is collected, making it still the most ticked box among all.

Given the fact that the most adopted VR/AR devices do not implement a GPS device (or similar) and that the users that consider their mobile device a AR device are a minority, this survey has revealed a bias: in the present time, most users assume

that a VR/AR device would collect their location probably due to the technological context in which we are.

On the other side, head movement, hand movement and eye movement are the data that are mainly collected by VR/AR devices and they have been selected by, respectively, 55.4%, 51.6% and 42% of the users. Given that these are the data that most of VR/AR devices in commerce need to properly work, this is a quite low response rate, showing that still a lot of users, including those who are aware of data collection, do not have a precise idea on how these devices work.

Finally, EEG data and heartbeat rate were included in the selection and only a minority of users would consider them as possible data collected, which are assumptions close to reality as, based on what emerged from literature review, only custom built VR/AR headset can collect EEG data and heartbeat rate can indeed be collected through most common VR/AR controllers but it is data that most application do not process (at the moment at least).

4.3. Confronting health, privacy and security opinion

Later questions revealed that, 38.8% of users had no concern about health issues, while 33.3% did not have any concern about privacy and 32.7% of users felt the same about security when using their VR/AR devices.

However, in the following questions they were asked to express their opinion over the same issues if they knew that they would be exposed to health, privacy or security threats by their devices.

The following are the answers received to these questions:

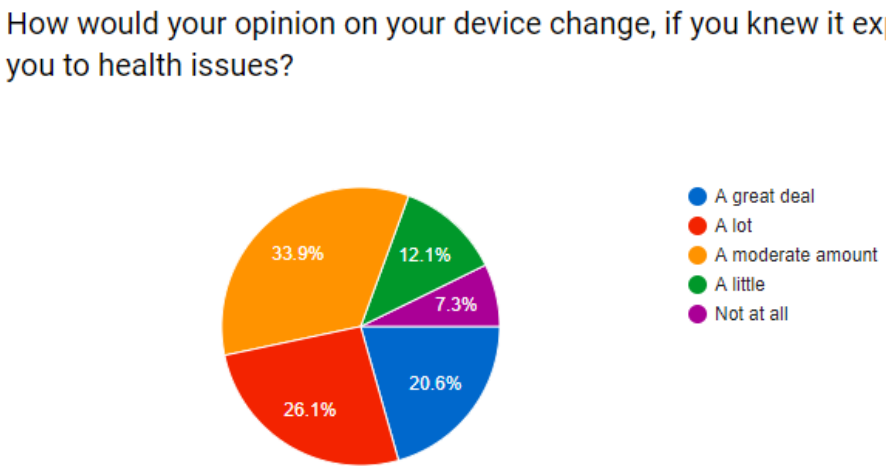

Figure 7. Influence of health issues on VR/AR product perception

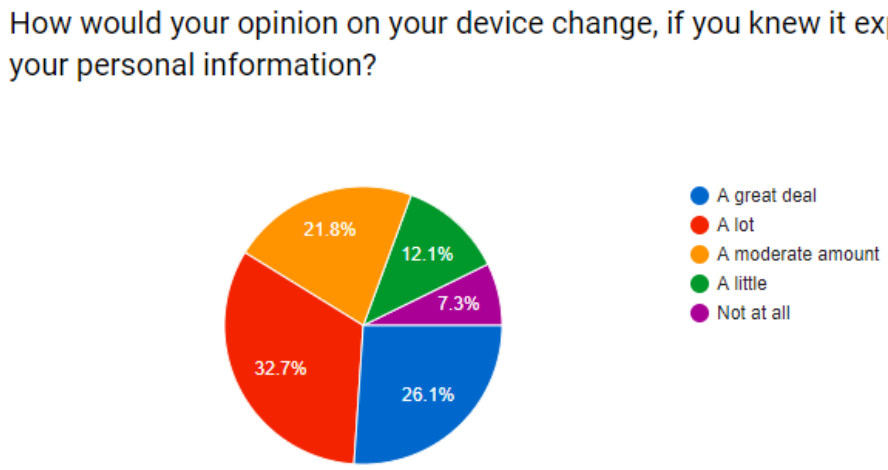

Figure 8. Influence of privacy issues on VR/AR product perception

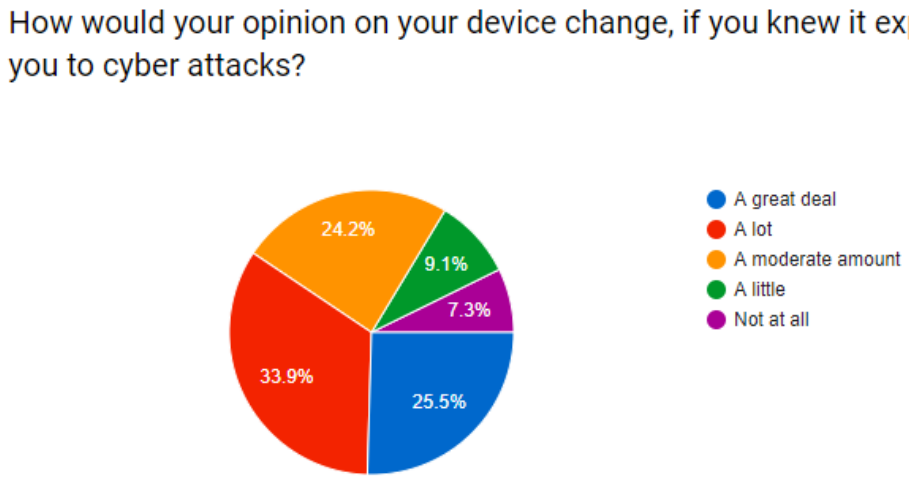

Figure 9. Influence of cybersecurity issues on VR/AR product perception

As it can be seen from the graphs, the current opinion is based on the fact that the users do not expect such problems to incur. This trend is against the information retrieved through the literature review [15], in which the results seemed to be that these issues more than developer. From this confrontation emerges the opposite and the conclusions in the following section over the interviews conducted with industry experts will confirm this discrepancy.

4.4. Interest over data collected and product category

The questionnaire confirms the growth potential of VR/AR technologies. As the graph below shows, 72.2% of the users are likely or very likely to suggest VR/AR technologies to friends.

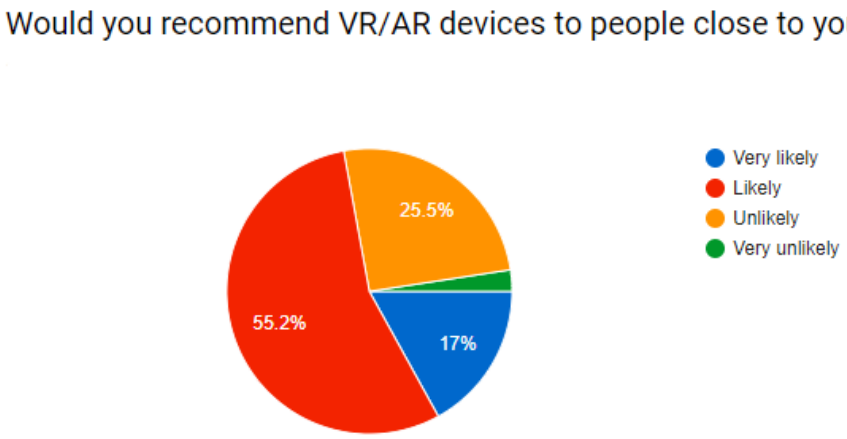

Figure 10. Rate of users that would recommend VR/AR products to others

This trend was seen already in literature [15], where the survey resulted in 5 out of 10 users likely or very likely to spread and only 2 out of 10 expressively saying they would not recommend it. In this case, the result is similar as there was no possibility to give a neutral reply and, consequently, there are more negative opinion but still greatly outweighed by the positive ones. In the beginning of this chapter a positive correlation, between the user experience and their willingness to share their experience, was anticipated.

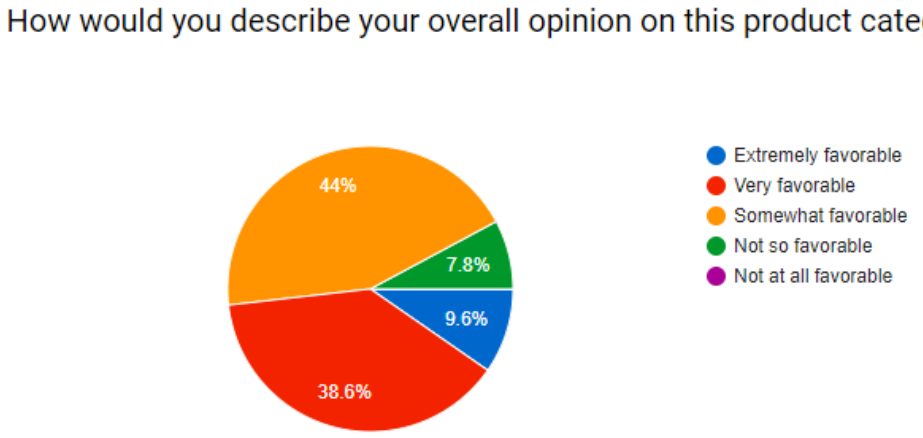

Figure 11. Opinion of the users on the product category

Again, it is intuitive to think that a user that had a good experience is more willing

to share the same experience, however it must be noted that, based on the statistical data observed in this survey, the correlation is not too strongly positive; this means that also those who are not entirely favorable would suggest the experience to other users. It is also important to notice that no one declared him/herself not at all favorable to this product category, which per se demonstrates a great willingness of the market towards the product, provided that the issues expressed are solved.

This last hypothesis is corroborated by the last question, represented in the following graph:

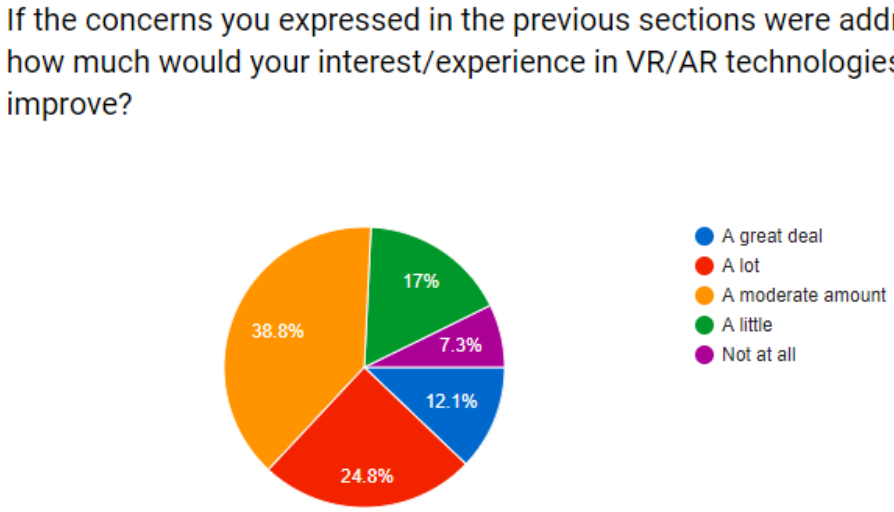

Figure 12. Impact that addressing the concerned expressed would have on VR/AR product perception

38.8% of users said that their opinion would have changed a moderate amount, 36.9% said that addressing these concern would definitely impact their experience (sum of a lot and a great deal) and only 24.3% said that it would have had little to no impact (sum of a little and not at all). Again, it is possible to see that these concerns do impact the experience and that users are looking forward for a change.

Finally, despite the concerns expressed in previous sections, as figure 13 shows only 3% of users said about data collected by VR/AR devices that they were more concerned than with other devices. The majority of the users (63.3%) declared themselves interested in data collection without distinction of technology, while 12.7% declared themselves uninterested without distinction.

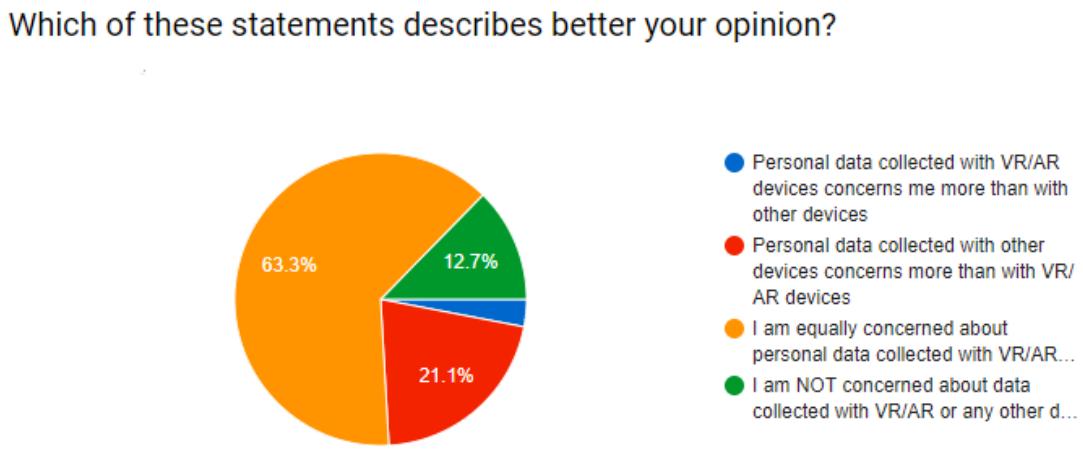

Figure 13. Impact that addressing the concerned expressed would have on VR/AR product perception

One in five users (21.1%) is more concerned with data collection with other technologies, although this might be due to lack of information, as the following question (figure 14) revealed that 39.1% of users are very interested (some of them extremely interested) in the data collected through VR/AR devices:

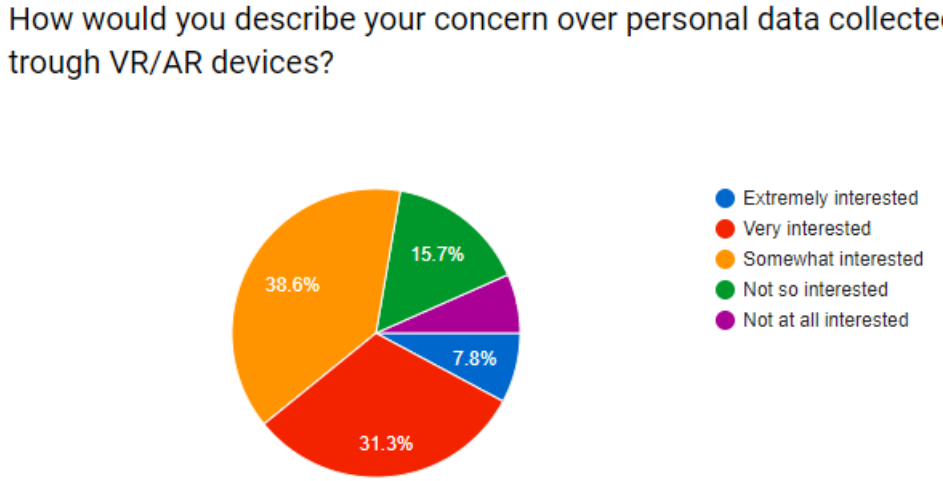

Figure 14. Impact that addressing the concerned expressed would have on VR/AR product perception

21.3% of users in total said that they are not interested or not at all interested in data collected through VR/AR technologies, which is not too far from the 33.8% total users that in the previous question declared themselves more interested in data collected by other technologies or not interested at all. Overall, the vast majority of users has

interest in how data is collected, although it seems that other technologies are more concerning for a large part of users. We can thus conclude that the misinformed user are more probably such due to miscommunication on the developer side rather than because of lack of interest on the user side.

5. Results from interviews

The interview with industry experts have been conducted with a semi-open structure, as previously mentioned in methodology. The pool of candidates was selected among people with experience with VR/AR technologies but not only. In order to have a wide array of opinions, three main traits were searched for: technical knowledge of software development and networking, business development experience (even minimal was accepted) with VR/AR technologies, cybersecurity knowledge. Ten candidates were approached and, depending on their expertise area, the interview was conducted focusing on some issues (ethics, operations, security etc.) so to have the most pertinent and valuable contribution out of all. None of the interview lasted more than 30 minutes and all the talks were recorded, however all the candidates accepted with the guarantee that their identity would have not been disclosed in this dissertation (or in other forms). For this reason the identity of he candidates will be kept secret, however the final pool composition can be graphically represented as follows:

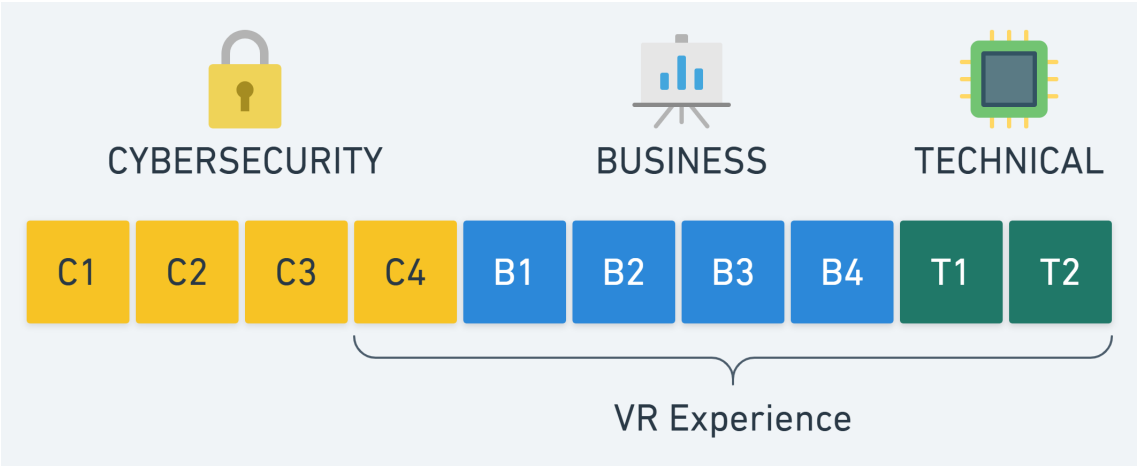

Figure 15. Graphic representation of the experience of the candidates selected for the interviews

As the image suggests, the majority of the 10 candidates were selected with cybersecurity and business experience. Moving on any comments made by a specific individual will be pseudonymized as the image suggests: C$\varkappa$, B$\varkappa$,T$\varkappa$ are used as shorts for Cybersecurity$\varkappa$, Business$\varkappa$, and Technical$\varkappa$. This will allow to keep intact the privacy of the candidates while showing also what was the background of the quoted expert.

From the interviews many sensibilities and many opinions emerged, what follows is a summary of the main topic discussed and the prevalent suggestions offered. In some cases comparison with literature review will be offered. This because in some cases the candidates were confronted with individual questions regarding a precise theme, with reference to the previously reviewed literature, to which they answered corroborating, or contradicting, the assumptions made on the base of reviewed literature. Intuitively, the candidates with technical background received custom questions on technical issues and the same logic was applied with all the others.

5.1. State-of-the-art elements for a secure lab, Gap analysis

The , were made to identify a a "state-of-the-art" environment, under both physical security and cybersecurity perspectives, to conduct research and collect personal data with VR/AR applications. In order to put at use, and test the feasibility, of the suggested methods the "TalTech Re:creation VR First" [36] lab was used. The premises of the "TalTech Re:creation VR First" [36] lab consist of a room with many VR devices, a discrete number of working station and a 5x8 meters free space in which users are usually invited to test and use VR equipment for various purposes.

As B3 suggested, in order to create a "state of the art" environment, we first have to establish a purpose for the environment itself, this will allow to identify which resources are more important and require more attention and which will not. For the purpose of this research, it was assumed that the "TalTech Re:creation VR First" [36] lab main objective is to have 10 to 50 users every month to use VR equipment for 30 to 60 minutes, collecting personal data[11] that can subsequently be retrieved from a server for research purposes. With this setup in mind, a few gaps emerged between the ideal environment and the actual environment at hand, in particular:

- lack of cybersecurity policy

[11] We assume that all the aforementioned types of data (EEG, body motion, eye track, hands movement etc.) can be collected without following a specific procedure. Follows that there is no limitation on the number of sensor/software put together at the same time except that at least one relevant device (from the privacy perspective) is used for each test. This way, we assume that the sessions can be discontinuous from the perspective of data quality and quantity but not from the security perspective, as it is axiomatic that during each session personal data will be collected and stored.

- lack of GDPR policy
- lack of efficient and secure data flow structure

To solve the gap, firstly were used the results emerged from a preliminary research on the web and the interviews with experts in the field, from which emerged that the key to a secure design would have been implementing a multi-layer security framework and sacrificing accessibility over integrity and confidentiality if possible. The biggest trade off would clearly be in such a scenario: how to have data transmitted securely with acceptable latency?

The value of "acceptable latency"[12] was devised based on literature [64, 65]. According to Bernier [64], below 100 milliseconds the latency is acceptable for 3D applications that are communicating with cloud server, however Raaen [65], has made a comparative study that shows that, due to possible input lags and other factors that a developer should account for, it is better to consider acceptable a latency value that stays below the 45-60 milliseconds. Considering that Chenechal and Goldman [66] have shown that on HTC Vive has a latency input-display of 30 milliseconds with 3D apps, while Raaen and Kjellmo [65] have shown that Oculus has an average latency of about 20 milliseconds on the same trip, we will consider acceptable a network latency that is below 20 milliseconds, so that the total of input and network shouldn't be above 45 milliseconds.

According with T1, a "standard practice" for small environments in this industry is sending data from a host machine to a server running on a virtual machine. For this reason, some online literature was examined and the following comparison emerged. The table below summarize the benefit of taking a server on a virtual machine over having it in a physical structure, as stated by Nakivo [2], an international data protection consultant:

[12]Latency is the time that occurs between input and output; as this definition is very generic, for this section it should be considered that the latency aimed to be reduced is the one the intercourse between a user's input with controllers and a graphical output on their VR device. It should be kept in mind that the many "hops" between the movement and the image resulting displayed are summarized and simplified in the following section as "network latency" and " input latency".

Table 1. Differences between a physical and a virtual server [2]

Physical Servers	**Virtual Machines**
Large upfront costs	Small upfront costs
No need for licensing purchase	VM software licenses
Physical servers and additional equipment take a lot of space	A single physical server can host multiple VMs, thus saving space
Has a short life-cycle	Supports legacy applications
No on-demand scalability	On-demand scalability
Hardware upgrades are difficult to implement and can lead to considerable downtime	Hardware upgrades are easier to implement; the workload can be migrated to a backup site for the repair period to minimize downtime
Difficult to move or copy	Easy to move or copy
Poor capacity optimization	Advanced capacity optimization is enabled by load balancing
Does not require any overhead layer	Some level of overhead is required for running VMs
Perfect for organizations running services and operations which require highly productive computing hardware for their implementation	Perfect for organizations running multiple operations or serving multiple users, which plan to extend their production environment in the future

As this comparison shows, taking the server on a virtual machine offered a good degree of accessibility and would have allowed a swift communication between the application and the server even with a strong encryption implemented between the two parties, as proven by the network test done, of which the proof is given in the following images:

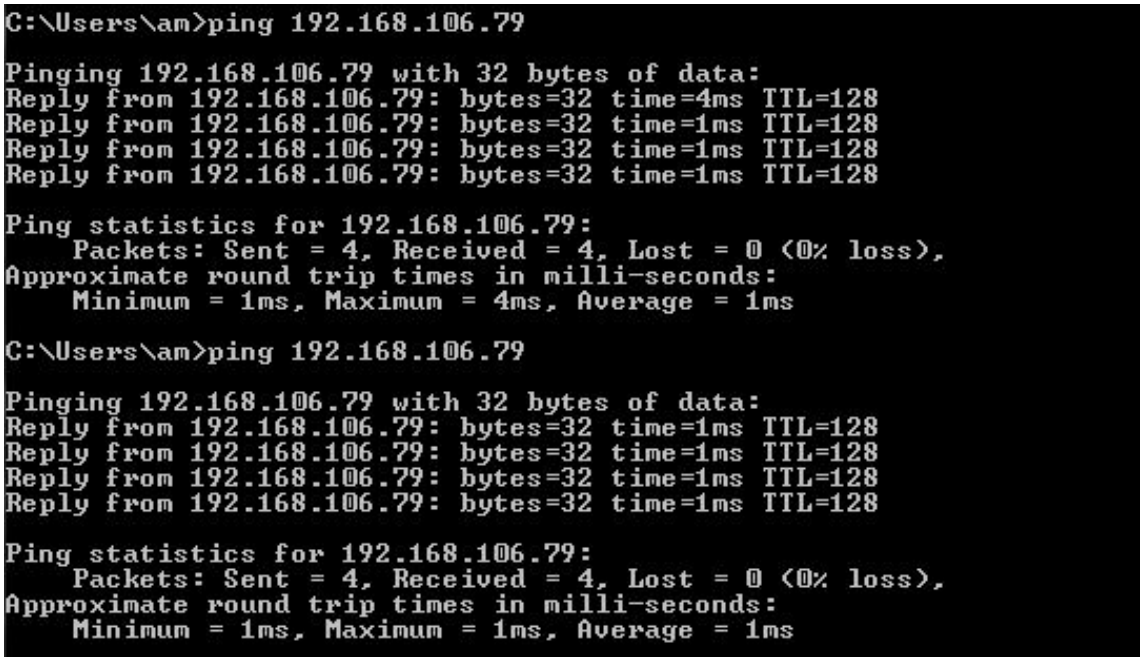

Figure 16. Ping test between two different Windows machine in the same network

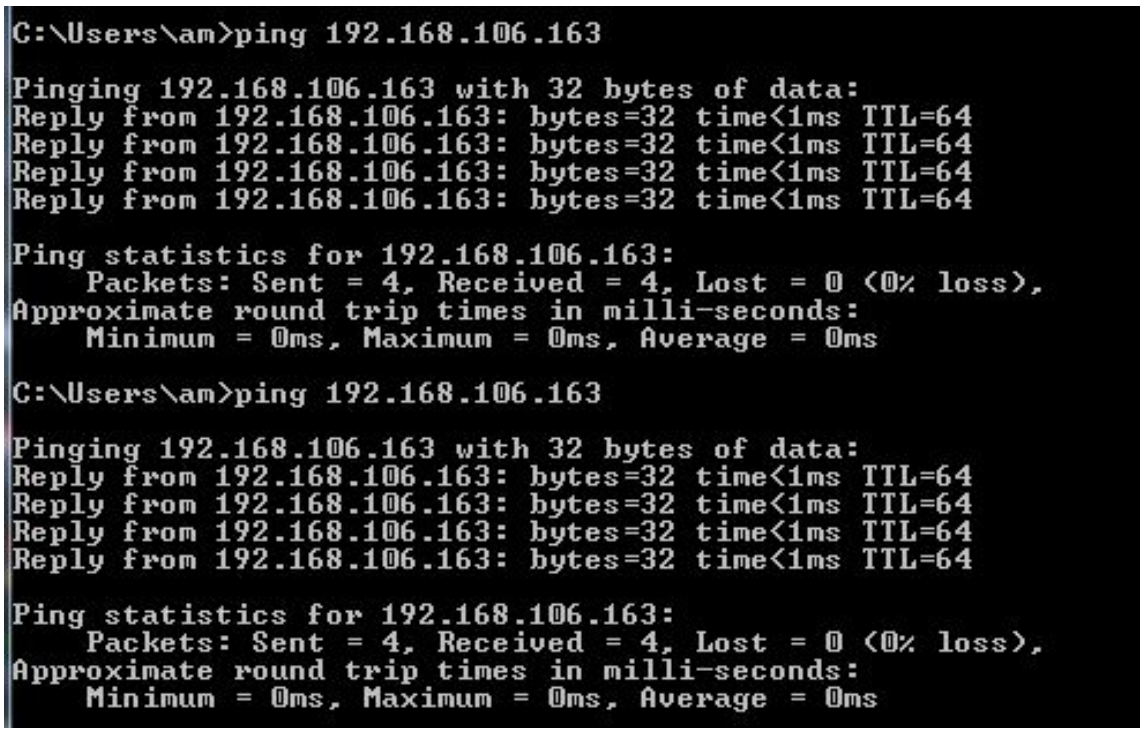

Figure 17. Ping test between Windows host and Ubuntu Virtual Machine

As can be seen in figures 15 and 16, both cases showed a very low latency, however in the case of figure 16 (the test between virtual machine and host machine) the results were slightly better (close to 0 milliseconds of latency).

To increase accessibility, a third party service (InfluxDB) was chosen to store the data on a cloud server. The data would then be accessible from anyone (provided that the credentials are in check) and this approach would add an additional layer of security to the structure, as to retrieve the data an attacker would have to have both access to the decryption key and the information on the cloud server.

With the hardware structure in place the trade off shifted towards using TCP connection versus UDP. TCP connection between host and virtual machine was eventually chosen due to the followings:

- TCP uses checksum for error control
- that due to the above TCP is more reliable when transmitting encrypted data
- that there is more literature and support for application that implement SSL and TLS over TCP

Finally, the service for the third party cloud database was needed. Based on the data provided by SolidIT [63], an experienced consultant with focus on database application and software development, four best candidates (among open source) emerged. Here follows an evaluation of their strength and weaknesses:

1. Mysql: ranked as best among the open source Relational DBMS, and second overall [63]; developed by Oracle in 1995, this database has a secondary model that can effectively serve as document store, it uses C and C++ as implementation language and its server side can work on any operating system it supports many programming languages among which: Ada, Delphi, Eiffel, Erlang, Haskell, Java, Node.js, OCaml, Perl, Python, Ruby ,Scheme, Tcl. It does not implement a simple rights management system.
2. InfluxDB: developed in 2013 and ranked as the best for "storing time series, events and metrics" [63], it supports a simple right management system (users can access through an account and the rights they have are defined by the account type). It supports a wide array of languages although not as many as Mysql and is also based on a schema-free version[13]. It only supports Linux and OS X.

[13]Schema-free databases can be considered more flexible as they allow the creation of documents without having to define a specific structure for them first. There are benefits of using databases

3. Elasticsearch: ranked first among the services that implements a Search Engine model as primary model [63]. Elasticsearch supports only a few programming languages (.Net, Groovy, Community, Contributed, Clients, Java, Perl, Python, Ruby). It was developed in 2010 and it can run on any system provided that it supports a JavaVM. Like InfluxDB is schema-free and offers a role-based access control with advance commands, although it requires additional setup of Kibana in order to fully take advantage of these functionalities.

4. MongoDB: first released in 2009 is ranked as best for document storing [63]. it can run on the most used system (Linux, Windows, OS X and Solaris) and is schema-free. It supports all the programming languages of the other counterparts plus many more. It implements a simple right management and can use a search engine secondary database model.

Due to the its favorable properties, InfluxDB was chosen, as it was clearly the best fit[14] for the desired lab structure.

The application used to transmit the data is Unreal Engine 4 (version 4.23) [67]. In order to send data through TCP connection we availed ourselves of the guidelines provided by T1:

1. SocketIO plugin: https://github.com/getnamo/socketio-client-ue4

2. Instructions for setup from Egor Bogomyakov[15]: https://medium.com/@slonorib/how-to-connect-unreal-engine-4-to-local-server-via-sockets-9d73fd180f0b

The interviews with experts in the sector revealed in multiple cases (T1, T2, C2, C3, C4) that selecting a open source software is a more desirable approach for my case.

(such as Mysql for example) that implement schemas, however for the purpose of this general comparison schema-free databases should be intended as more flexible system as they can at least theoretically be adapted to more situations.

[14]Taken into account the scope of the lab, a Time Series DBMS seemed to be a better fit for our particular case, although it is not to be excluded that for other VR application purposes any other of the quoted services could prove a better fit. The comparison showed before is to be intended in a non-exclusive way as certainly for other researcher it can be useful to know the various differences among the services in order to chose a best candidate, which should not be necessarily InfluxDB

[15]This guideline on how to setup the plugin does not include the implementation of OpenSSL encryption. Documentation explaining how to implement it is referenced in the link SocketIO plugin page (https://github.com/getnamo/socketio-client-ue4) but is not coming from the official developers. There are other plugins for UE4 that might have an easier implementation of encryption protocols, however for simplicity (and due to the kind cooperation of the developers involved in this project) this is the guideline used for this project

Given the fact that we do look for a safe structure, based again on interviews (C2, C3, C4) more than literature, SSL encryption was implemented for the data transmission between the host application and the virtual machine, as encrypting the data that goes from application to server would impede any relevant breach of security in case of spoofing attack (data that gets collected in the internet communication between application and server). In order to understand the impact of security over accessibility, a comparison over the registered network latency before and after implementing the encryption was made and the followings are the registered results:

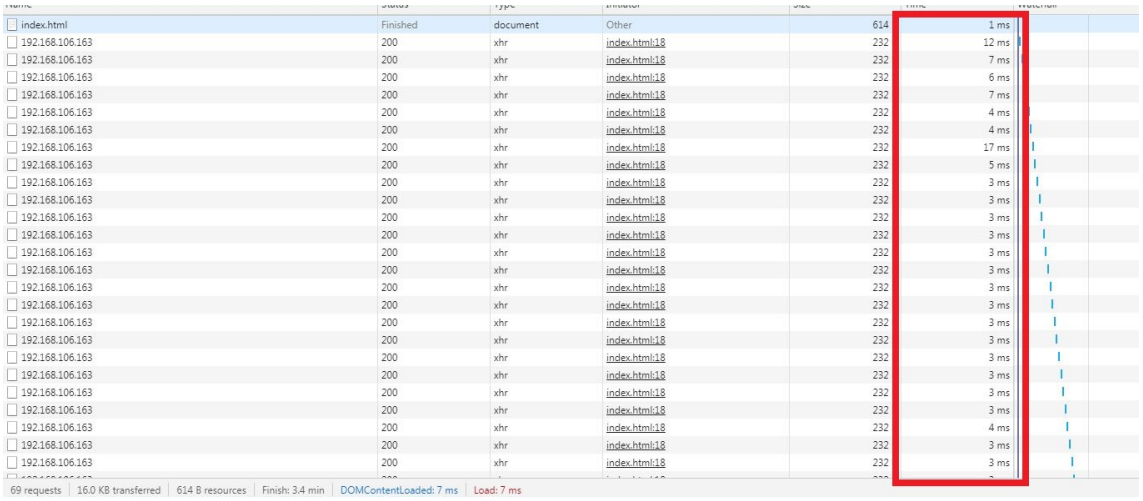

Figure 18. Sending packet without encryption test

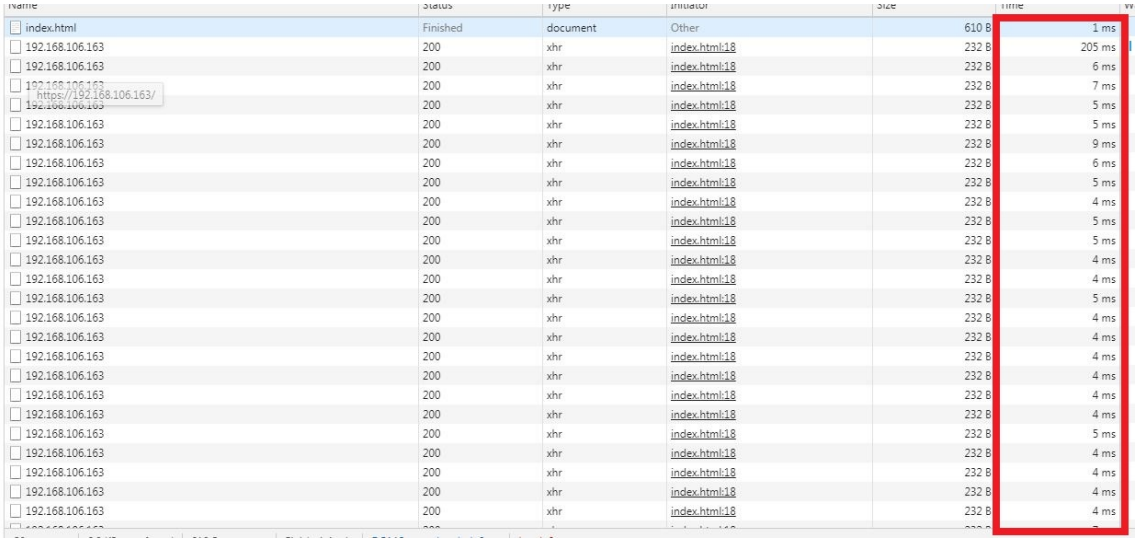

Figure 19. Sending packet with encryption test

As it is also evident in figures 17 and 18 show, the latency is lower without encrypted connection. However the latency value shown is way below the 20 milliseconds limit

that was mentioned before; for this reason, implementing encryption is a feature worth its cost in terms of delay.

5.2. Data privacy

Section A1 and A2 of the interview required the candidates to talk about privacy issues encountered while dealing with personal data. The results of the survey already show a broad interest among users for what concerns the problems of privacy and security. Out of 10 interviewed people, 6 replied that they relied on third-party services to store personal data, while 2 revealed that they kept and processed data on premises following GDPR guidelines. Of all the candidates only 1 had problems in the implementation of policies within the company due to inability of the personnel to understand the value of PII (C3), and only C1 felt like the users, independently from the effort a developers put, are still not aware enough of the value of their PII. Thus from the interviews I can conclude that the attention to this matters is even more alive in the developers' mind than in the users' as no one of the interviewed candidates was uninterested in such themes and, on the other side, some strongly expressed the intention of evangelizing the attention for PII.

As B2 noted, in fact, a privacy policy should be in place regardless of whether or not a user considers his or her data valuable and the user should always be informed properly of the data that is collected and the purpose it is used for. It is necessary to design a structure that by design does not allow personal info to be divulged. Also the existing legal framework had to be taken into account. GDPR already compels data collectors and processors to ask for permission and ensure the safety of the data. For this reason, the guidelines are integrated with some research over the current EDPB Guidelines [68] and the GDPR [69] requirements to collect process and store PII.

It suffices to implement a template [70] retrieved from the official GDPR website as a first measure. Given what emerged in the literature review, a review of k-anonymization process was made too. Given the nature of the activity to be conducted in the lab, data publication is to be included as an eventuality; in such case, preserving the complete anonymity of the test subject is of paramount importance. The question that emerged was"given an acceptable level of information loss, what value of k should be used to guarantee higher privacy" [71]?

Given that "a minimum k value of 3 is often suggested" [72], and that the higher value of k the higher the issue of data perturbation [41, 42, 73, 40, 39, 37]. This means that in a hypothetical data-set containing personal information such as movement

tracking, a research for any combination of attributes would give at least 3 identical results. In this context some useful guidelines to apply this level of anonymization can be:

- Suppression method should be applied to names of the candidates
- Generalization method should be applied to age and region of the test candidates
- Other sensible information, such as gender of the candidates, that cannot be subject to generalization, should be mark as such to inform the candidates of the risk and, possibly, the opportunity to not specify such information should be given

Successfully implementing k-anonymity with a value of 3 for K ensures that is impossible, for an attacker that does not posses already the majority of the information of a candidate, to uniquely identify someone based on the data published, as demonstrated also by Yang Xu [42].

In the regards of other matters emerged during the interviews, all the candidates (regardless of their background) showed a deep understanding and interest in the current data regulation, only C1 expressed the inability of being fully compliant but not due to lack of knowledge or effort. As stated by C1, "everyone working in the sector of biometric authentication can never be fully GDPR compliant. If data is anonymized on our server but, for example, the usernames on the servers of the institution we provide a service for are not, then the anonymity cannot guaranteed anymore. In a worldwide context legal inconsistency makes it hard to achieve anonymity". A particular remark that shows that, in some cases, is not the lack of effort of a developer as much as the inconsistency of the international legal landscape that limits the control users have over their data. At least in industry that are emerging and rely on personal data, as C3 shared multiple experiences with non-innovative businesses that did not satisfy at all standards of data privacy awareness.

5.3. Ethical issues emerged

All the candidates were eventually confronted with ethical questions on matters spanning from cyber-bullying to mass espionage and social endangerment, exposed in the literature review. The intention was certainly not to find a solution to such big problems in their answers, but these questions over the greater good and the future of society forced almost all of them to take a few seconds to gather an answer. In the majority of the circumstances, when facing the greater problems that can be summarized with the question "would it not be better to put a stop to technological development?", only one of them (C3) asserted that it would have been the right thing to do, while the rest, in a way or another, opposed this scenario with the fact that "technological progress is necessary and neutral, it's the people that commits crime, not the technology", thus (knowingly or not) referring to that concept that in forensic language would be expressed as: "mens rea". "Depending on the jurisdiction's chosen approach, the perpetrator must have a certain "guilty" mental state, or mens rea, in order to be found culpable of this offense" [74], the totality of the interviewee seems to agree with this notion.

The concept of "mens rea" finds its roots in St. Augustine, while application of the same concept juridically can be found as early as 12th century [75]. It is a concept very much rooted in our society that has been certainly influenced by our Judeo-Christian culture [12, 75]. It is essentially the presumption of liability.....none of the interviewed considered himself/herself liable for any wrongdoing that would have come from the misuse of technology they would have not been able to foresee in the first place; only one of them tried to pose a mild challenge to this idea by asserting that he would have tried "to at least know all the possible consequences of these new technologies", but still would have held himself/herself not accountable if any misuse was made outside these boundaries. All the other interviewees simply assumed as "impossible to know all the possible implications behind the use of a piece of technology", reinforcing the idea that "actus reus non facit reum nisi mens sit rea" (the act is not culpable unless the mind is guilty) [76] .

Although this is an understandable point of view, during the interview the candidates were challenged on this notion going into the deeper roots of their ideology to assess how solid was the conviction of non-culpability; on multiple occasions (C1,C3, C4, B1, B2, B4) the interviewee replied with the common saying that "it is not possible to know all the consequences of our action" and B4 even remarked that "regulations

are written in blood", thus implying a necessity for humans to experiment at their own risk.

On this point, it is due to dive deeper in the question of ethics and responsibility; although the *mens rea* concept has been a fundamental block in the judicial system of our western society and not only, as there are traces of the same concept outside the western cultures, in the present days the notion that guilt depends on the "guilty state of mind"[77] is being challenged by many [12, 78, 79]. It seems that modern philosophy and psychology dares to challenge the common notion of "good will" putting it in perspective of the political events of the last century and, more important, under the perspective that today we are "unfree and chained to technology" [80].

Ethics is the philosophy of the ἔθος (from Greek: costume, habit), it should thus change as our habits change and the philosophical understanding around the sames evolves. Having to put under question the ethics of the technological habit evolving through VR, an ethical evaluation cannot prescind from challenging the "neutral[...]essence of technology" [80]. In doing such, the interviews revealed how scarcely the

It seems that, as the Socratic philosopher charged themselves of finding self sustainable truth that would resist against rhetoric challenge, in modern context cybersecurity is charged to find the "ἐπιστήμη" [81] (episteme[16]) of a technological structure: a self sustaining design that by itself is sufficient to eliminate proneness to failure. It is due to challenge common notions of ethical behavior and verify how much they contribute to a cybersecurity framework which modern guidelines require to be "secure by design" (self sustaining, epistemic).

Max Weber said that a man is "guilty only as far as the actions are foreseen" [82] and most of candidate seem to abide to this logic, almost as if they would take it for axiomatic truth. Thus, follows that the it would be quite a shock to this axiom, emerged during interviews, to discover that everyone is accountable for the consequences of the misuse of a technology they developed, regardless of their original

[16]Episteme is, litterally, a self sustaining truth. Moving forward whenever this word will be used in a generic context it will have the valence of "self sustaining truth/assertion". The expression is a literal translation in latin characters of the aforementioned ἐπιστήμη. The term episteme is used not in reference to the philosophical, mathematical disciplines of epistemology in this context, but as its pure semantic relevance drawn from Socrate's dialogues. [81].

intention.

After the second world war, Karl Jaspers writes a renown essay called "The Question of German Guilt", identifying 4 key points of blameworthiness for the war [83]:

1. Criminal: for those who act in contradiction of a judicial framework
2. Political: for those who do not use their political power (as citizens) to oppose the facts
3. Moral: for those who decided to conveniently overlook the perpetration of injustice
4. Metaphysical: for those who survived the same injustice that killed another man

Applying this conceptual framework in opposition to the mens rea, would reveal a much deeper and disturbing context of guilt in which the interviewed candidates all befall with different degrees.

Some of them highlighted the awareness of operating with new technologies that the current legal landscape is not ready to face the sudden changes brought by the fast development of a ground breaking technology (a fact that lawmaker themselves have admitted in some instances [56]), making them Criminally and Morally guilt, as they act knowingly of the edge of legality and chose to make a convenient situation out of it.

Others realized that the "sacrifice of someone" would have been necessary to make the lawmakers aware of the dangerous aspects of this technology, enough to prompt a legal change. These persons could be considered Morally and Metaphysically guilty as they realize the necessity for a change but decide to let others be victim of accidents for their convenience. Some of them showed active interest into participating in the improvement of the user experience through technical efforts, others simply liquidated the problem of making people aware with "I will warn others about the risk and let them decide if they are ready to take them", de facto asserting that they would let a user (for how inexperienced he/she can be) assess by him/herself the degree of confidence he/she has with virtual environments. Could this be considered both Moral and Political guilt?

Raymond Boudon any decision made in a group to solve a problem, in addition to the expected and intended effects, may have unintended effects that "often cannot be determined intuitively". The collaborative result does not match the original intentions [84].

A demonstration that technological development has an impact on people that is all but neutral can be also drawn from the questionnaire; most of people expressed that their concern would change over VR/AR products if they knew that they would expose their information, but how does this combine with the fact that most users assume VR/AR devices track location when in fact the opposite is true? Might it be because people already surrendered to the idea that such data is being handled and, although they care for it, they feel like they have no control over it anymore? If this was the case, how should those who operate in this sector (at any level) consider themselves in light of this turn of events?

I work for progress, progress is good, my work is good. This seems to be the syllogism emerged from most of the interviews, which becomes a very fragile chain, like all syllogism, as soon as it is taken outside the logical sandbox in which it is conceived. "Act so that you treat humanity [...] as an end, never merely as a means" [85], said Kant back in 1785. But if today we assume that the only way to develop technology, such as VR/AR devices, is through the collection of personal data, and we then imply that progress is necessary we are basically implying that humans are a necessary mean to develop technology, subverting a fundamental ethical principle.

The conclusion over the ethical debate with the experts can thus be that there are at least 3 bias that should be overcome: that technological development is not just natural but necessary, that implying humans as means for it is necessary and that responsibility of an individual is defined by the will of the individual itself.

6. The research for novel approach

Modern Cybersecurity theory [74, 57, 19, 1, 3] has found out that hybrid approaches[17] are necessary to effective response to security incidents. Use of both quantitative and qualitative method is now common practice [19, 86], based on this literature and on the opinion of security experts, and on the philosophical and mathematical problem solving literature [12][87], a hybrid model to represent the VR/AR cybersecurity problem lifecicle was devised on both technical and ethical perspective; the model compounds a "a priori" and "a posteriori" solution techniques, that are based on "binary" or "routine" solution techniques and "non-binary" or "non-routinary" problem solving strategy. The need for this solution comes from the fact that, as it was recognized in the enunciation of this study's limitation, any solution that would be devised for the problems found in this research would probably not be resilient to the aggressive evolution of VR/AR products.

In order to mend this weakness, two solution stages were envisioned: an early approach and a late approach. In the early stages of the problem-tackling, a "a priori" solution framework can help find a quick response. However "such issues will require adapting existing doctrines to new circumstances" [56]. In the later stages of the problem-solving activity, a more multilateral approach is required, based on the new experienced gained ("a posteriori"). The main difference between the two stages is that while in the "a priori" approach the solutions are based on simplistic binary assumptions while in the "a posteriori" approach the novelty of the solution comes from the fact that there is no definitive checklist.

For example, let us take the case of a small lab trying to avoid a security breach; the lab consists of a machine behind a door. The door is either open or closed and if it is opened it must be closed. That is, in essence, the binary "a priori" logic. But, as often happens in cybersecurity, even when all the steps on the checklist are taken correctly there is still a data breach; for this reason in the following sections, a first structural model will be presented as a guideline to form a by-design secure environment. In section 6.3 however, a non-binary decisional model will be given as guideline to respond to unknown and unforeseeable cybersecurity threats. The same will occur in regards of the ethical issues.

[17] With hybrid approach we refer to problem solving techniques that compound qualitative and quantitative methods to analyze a phenomenon on multidisciplinary basis

All of the following models have been designed by taking into account the experience of the interviewed experts as well as suggestions from literature taken from more disciplinary fields (mathematics, law, psychology, informatics, philosophy).

6.1. Solution to the security issues

The solution of technical issues has been drawn by the assessment of the "state-of-the-art" structure plus the drawing of a security policy, resulted from the combination of both literature research and interviews. With the help of the interviews and the experience in "TalTech Re:creation VR First" [36], the following best-practice framework was drawn. It can be immediately applied by any business/researcher that works with a similar facility and has similar needs. The framework itself is a compound of previously tested solution that can be an immediate "first-aid" solution to pioneers in this sector. In the next section follows a description of what can be a good decision-making model to devise a more mature solution once the acquaintance with the problematic improves.

6.2. *A priori* solution

6.2.1. Lab purpose and data-flow

The purpose of the lab is to collect movement data through VR devices (HTC Vive and Oculus Rift). The data collected is to be considered biometric data. The data flow can be described as follows:

- Users wear HTC Vive/Oculus Rift headset are cable connected to a Windows 10 host machine
- On the same machine, an Unreal Engine 4 Application [88] runs, logging data outputted by the connected sources (eye movement, body movement, brainwaves, hand movement)
- The data is sent through a Socket.IO plugin to a NodeJS Server installed on Ubuntu Virtual Machine running on the same host machine.

- At the end of the session the data is uploaded to InfluxDB Database for cloud storage and processing

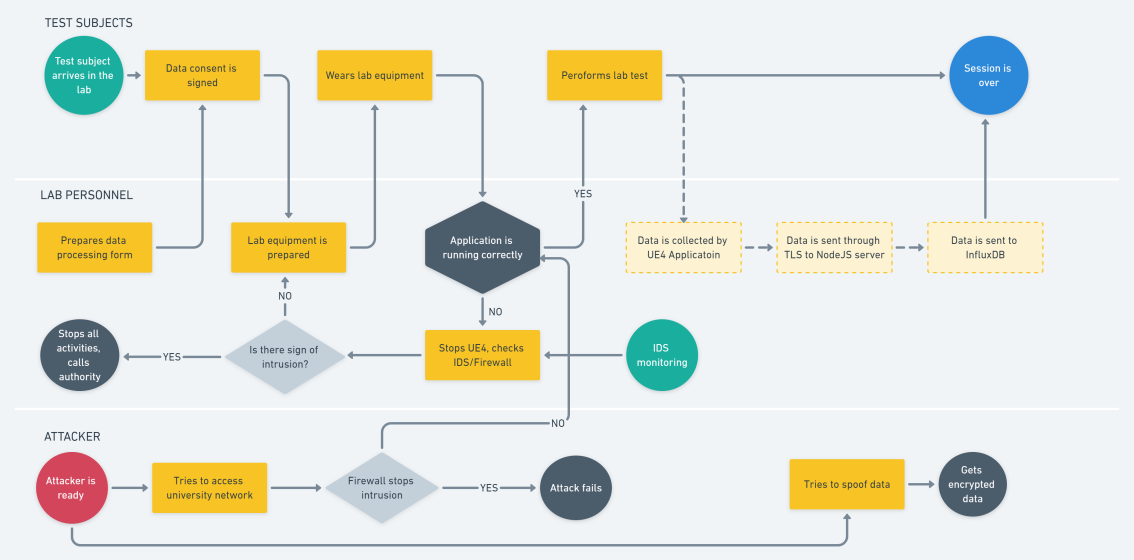

Figure 20. The workflow representation with attack vectors and data flow

In accordance with Estonian law the test subject that participate in the lab studies are required to sign a document in which they give a contact and allow the lab personnel to collect, store and process their personal data in accordance with GDPR official templates (https://gdpr.eu/data-processing-agreement/)

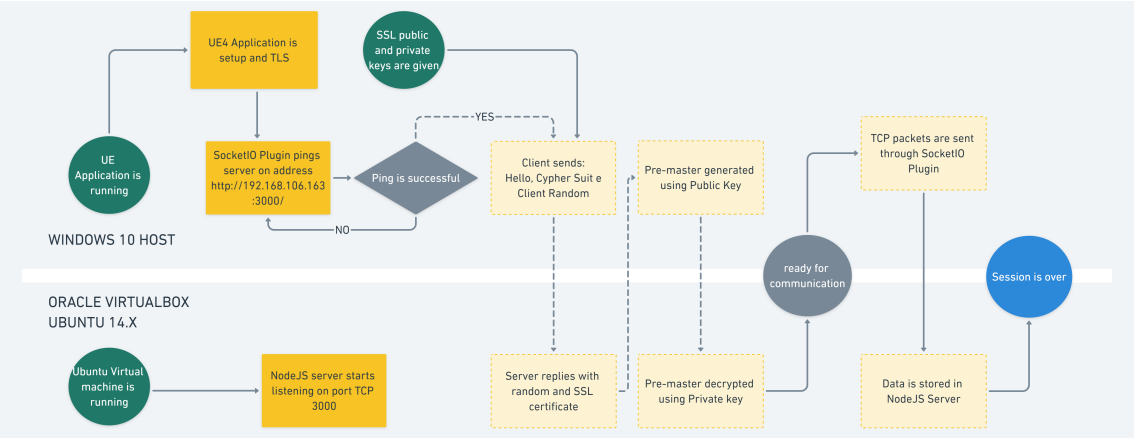

Figure 21. Representation of the flow of data between applications

As shown in the picture, spoofing and impersonation attacks are mitigated if not avoided completely by the implementation of encryption and IDS. Also in the case

of physical impersonation, the following procedures will add extra layers of security that require personal identification to access both structure and working stations.

6.2.2. Lab security features

At the setup of the premises the following characteristics have to be included in the structure design:

Physical:

- Logged access: all the entrances require access through a registered keycard; keycard owners are logged in the university system and to each keycard correspond a owner (keycard expires as soon as the owner is outside university network);
- Logged machines: no machine in the lab is portable and the most valuable equipment (headsets and working station) are labeled with stickers (logos, serial numbers et sim.) to be immediately identifiable
- Closed lockers: except for the drives in the working station, storage devices such as USB drives, SD cards and other lab equipment (headsets, cables, controllers) are stored securely in lockers that require access through key

Virtual:

- Logged access: to access a working station a password protected account is required, password for such accounts are electronically stored on a machine in a different location and can only be accessed by the lab owner
- Encryption: TLS encryption is used between UE4 Applications and NodeJS server - IDS software: Suricata is implemented both on physical and virtual machines
- CM Software: SaltStack is implemented as Configuration Management software on the Ubuntu Virtual Machines to more securely control the modifications and avoid tampering

- Firewall: all the machines (physical and virtual) make use of stock (non-custom) firewall software (Windows Firewall, Ubuntu Firewall)
- Cloud Storage: influxDB cloud server is used to securely store and access the data outside the lab

6.2.3. Lab security policies

After the setup, in order to maintain a safe environment the following procedure should be implemented:

- Training of the workforce: the lab personnel is aware of the criticality of the information handled and an update course is mandatory every 6 months over the cybersecurity in VR environment and data privacy laws
- Periodic check: once every week (Friday or earliest day available alternatively) the lab manager examines the log from the CM and IDS software, as well as the up to date status of the working stations and cloud services (InfluxDB)
- PenTesting: the human and technological weak points of the labs are assessed and tested at least once every year following emerging guidelines and cybersecurity cases
- Legal update: the data processing agreement is kept up to date and checked at least once every 3 months

6.2.4. Lab Incident response policies

Responding a breach in data the procedure to follow consists of:

Report:

- Local authorities are to be informed as soon as breach is noted
- The university CERT (Cybersecurity Emergency Response Team) is contacted within 1 hour of security breach detection (physical proximity to the CERT office makes physical contact a valuable alternative to telecommunication)

- InfluxDB dedicated security service is to be contacted and consulted within 2 hours (security@influxdb.com)

Assessment:

- Forensic data is collected through access log and software logs within 2 hours o Use of forensic tools (Autopsy et similia) to recover possible data loss and possible deleted logs within 8 hours
- An evaluation of personal data leakage is to be conducted and finalized within 24 hours, so that the affected personnel and test subject can be promptly notified through mail

6.3. *A posteriori* solution

The following is a best practice to set up a lab that can resist the future of cyber threats, however "existing tools are not yet adequate to provide cyber operation centers with highly desirable cyber SA capabilities" [19]. We must assume that, at some point, the structure put in place will not be sufficient. In order to keep it up to date, a decisional model that goes beyond the simplistic nature of the checklist must be implemented. In order to assess an unknown threat from a outside-the-box perspective, the solving strategies used in mathematical non-routine problems were reviewed.

"Non-routine problem solving can be seen as evoking an 'I tried this and I tried that, and eureka, I finally figured it out.' reaction" [89], it's a problem solving approach that implies numerous attempts and the exploring of different solution. In cybersecurity it is a practice that has been explored already [19], not surprisingly as routine activities are just as important as the ability of dealing with "zero-day" threats [90]. A non-routine problem solving model to be implemented was devised, taking inspiration from literature, and making adaptations to make it more fitting to the case at hand (small environment that deals with personal information).

"Defining what is in and out of scope makes it clear to all parties involved what will and will not be done" [8], so the first action to perform non-routine problem solving

is to establish a course of action in which a strategy is applied to reach a solution. Among other models Rajivan cognitive tasks analysis seemed to be very clear and easy to implement [1]

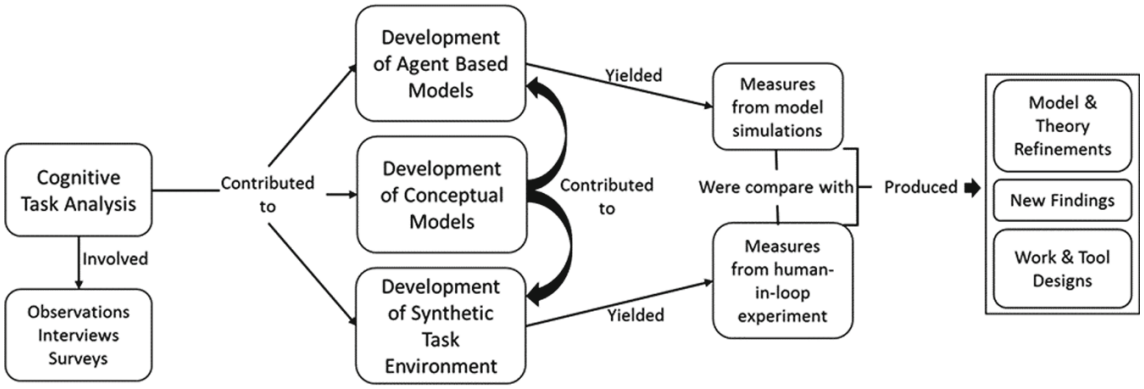

Figure 22. A Cyber Situation Awareness Hybrid Approach Model, source: Rajivan, Prashanth, Impact of team collaboration on Cybersecurity Situational Awareness[1]

However, this model was designed for bigger structures as it requires a large pool of experts, so a more generic model, such as the one developed by Zhong et al.[3] in a cognitive study, would have been better for a guideline. What follows is the comparison and explanation of the AOH and OODA models (Action Observation Hypothesis and Observation orientation Decision Action); on the left, the steps of the decision making process, on the right an explanation for each step:

Table 2. Cognitive model for decision making in ambiguous context, source: Zhong et al., Studying Analysts' Data Triage Operations in Cyber Defense Situational Analysis [3]

OODA	AOH	Description
Observation		The observation in OODA refers to the raw information which is presented before analysts' involvement. This data is captured in the Observation component in A-O-H model
Orientation		Orientation in OODA is "fusing information to build situational awareness)" [48]. This essentially incorporates the observation and through hypothesis cycles
	Action	The action performed to explore the monitoring data, to prove or disprove each hypothesis. These actions will result in new observations
	Observation	The observation of some interesting data resulted from actions. The collection of data may trigger analysts' new hypotheses
	Hypothesis	The thoughts generated based on the current observation. It could be an interpretation of current situation, questions in mind, or attempt to future actions
Decision	Hypothesis	The results of analyzing all hypotheses will result in a final decision. This is essentially the confirmed hypotheses of the A-O-H model
Action		Occurs after analysts' analytical reasoning processes and is thus not within the scope of the A-O-H model

In this model we see a comparison made to show the steps that are optimal in Cybersecurity SA[3]. Given the nature of the environment taken in consideration for this dissertation (small environment with 1-3 persons dedicated to security tasks), it seemed appropriate to adapt the model to a smaller, quicker response team but keeping the same main steps, which are resumed in the following table 3. In the first two columns of the left side, the AOH and OODA steps followed by the new model OHA2 (Observation Hypothesis Action Observation Hypothesis Action); on the right

a short description for the steps of the new model :

Table 3. Comparative vision of Zhong et al. models [3] with new OHA2 model applied in hypothetical context

OODA	AOH	OHA2	Description
Observation	Observation	Observation	The team observes the information collected by the security tools and the evidence found on the site
Orientation		Hypothesis	First hypothesis cycle over the causes of the Cyber Situation
	Action	Action	"The action performed to explore the monitoring data, to prove or disprove each hypothesis. These actions will result in new observations"
	Observation	Observation	"The observation of some interesting data resulted from actions. The collection of data may trigger analysts' new hypotheses"
	Hypothesis	Hypothesis	"The thoughts generated based on the current observation. It could be an interpretation of current situation, questions in mind, or attempt to future actions"
Decision	Hypothesis		
Action		Action	The final decision over the 2 hypothesis cycles is taken

As it is can be seen, the OHA2 (Observation Hypothesis Action Observation Hypothesis Action) structure is more empiric than the OODA/AOH model as it relies on multiple rounds of observations and actions. This decision is due to the fact that in case a small structure is handled, empiric test can be carried out in less time, thus quickly generating more results that can either lead to a conclusion or produce more evidence to be observed in following hypothesis cycles. A smaller environment also means less sources of evidence and, probably, less possible attack vectors; for this reason an action based model, rather than a hypothesis based or survey based, like the one made by Rajivan [1] et al., is more efficient for the purpose of this research. Nonetheless, this comparison offers a broader landscape over the non-routine problem-solving models that are being developed in cybersecurity research.

7. Solutions to the ethical issues

Let us assume that the words of the interviewees would have corresponded (theoretically) to their present action. In such scenario, building an ethical framework to aid them in taking an ethical choice with the "mens rea" judicial model in mind would add very little value to the ethical considerations already made.

To give a demonstration, here follows a "mens rea" judgment model, in which the interviewees ethical responsibility is judged based on what their intention is and on how much their action is safe, in accordance with the current legal framework, on a scale from 1 to 5; in this scales 1 corresponds to complete conviction of not being harming anyone (from the intention side) or absolute abiding of the effective law (from the legal perspective), and 5 corresponds to clear harmful intention (from the intention side), or disobedience to the law (from the legal perspective). In this model the moral responsibility arises when someone (obviously) commits an action against the law or with the clear purpose of harming someone else, but also when the intention is neutral and from the legal point the action is disputable (on a Cartesian plane it would have values of 3,3), like in the image below where the value that assigned to all the interviewees based on their replies is represented on a Cartesian model.

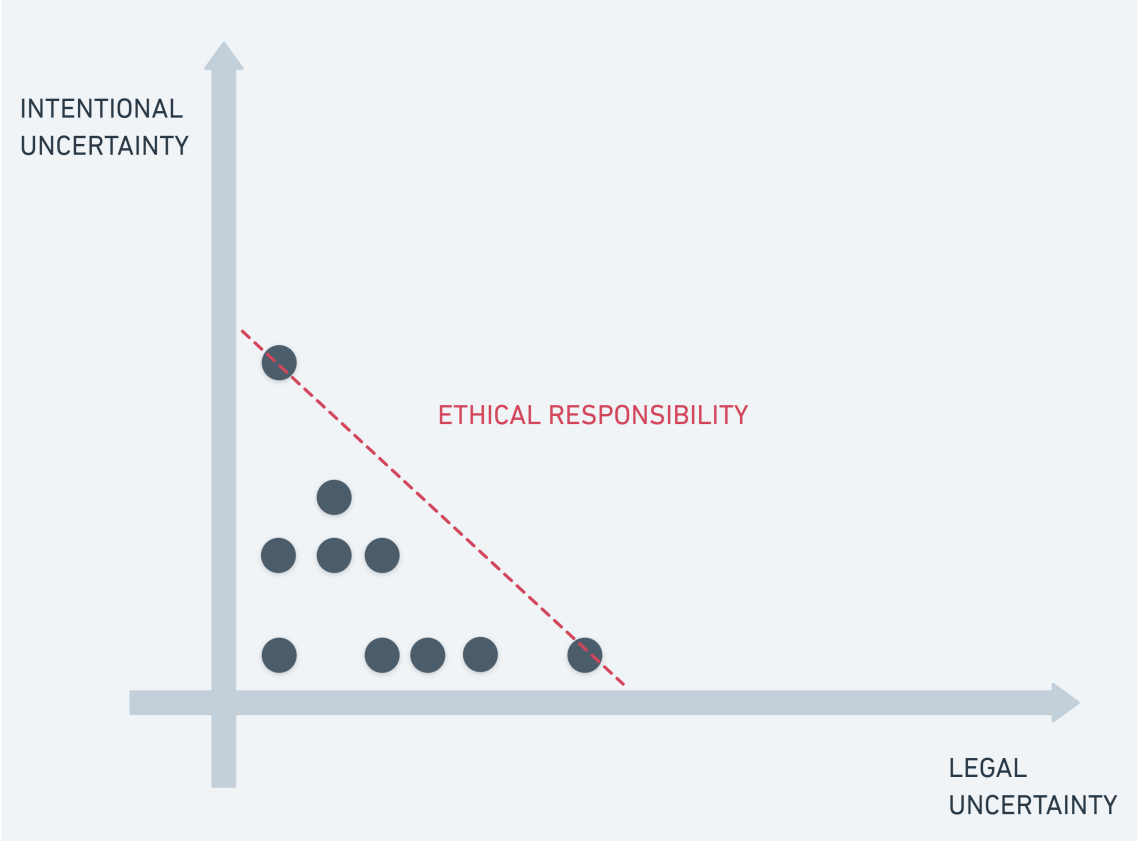

Figure 23. A "mens rea" conceptual model of the interviews conducted

As it can be seen, most of them are below the line and had positive intentions, some of them were not sure of the outcome of their actions but showed great interest in giving a positive contribution to the environment around them. From this perspective there is little than should be done on the ethical side, which is why the common sense emerged from the interviews should be challenged more strongly."[N]eutrality view on technology is untenable" [53]. Both the technical [53] [84] and social literature [79, 78, 81, 12] seem to converge over this point. The cause is that our ability to technologically develop is, at the moment, far superior to our ability to foresee the consequences of our actions [12]. If in this scenario we consider ourselves accountable exclusively for the consequences that we are capable to foresee, than we will conveniently realize soon enough that those consequences are a minority of the possible outcomes. The "mens rea" solution, at least on the ethical side, is not sufficient anymore to push modern developers towards a greater responsibility.

7.1. *A priori* solution

Jacques Ellul asserted that "ambivalence" is an intrinsic, inseparable characteristic of how technology is developed." "technology cannot be considered in any way other than simply as "good", "bad", or "neutral", but fully made up of a "complex mixture" of positive and negative elements" [84] that consequently develop into "unintended but foreseeable effects", "totally unpredictable" effects, or "unpredictable but expected effects" and "unpredictable and unexpected effects" [84]. With this mindset, we can try to envision a model that works a priori with new problem that can be immediately confronted with already existing solutions. In the next figure, follows a model that classifies the most notable problems emerged through the interviews with the experts.

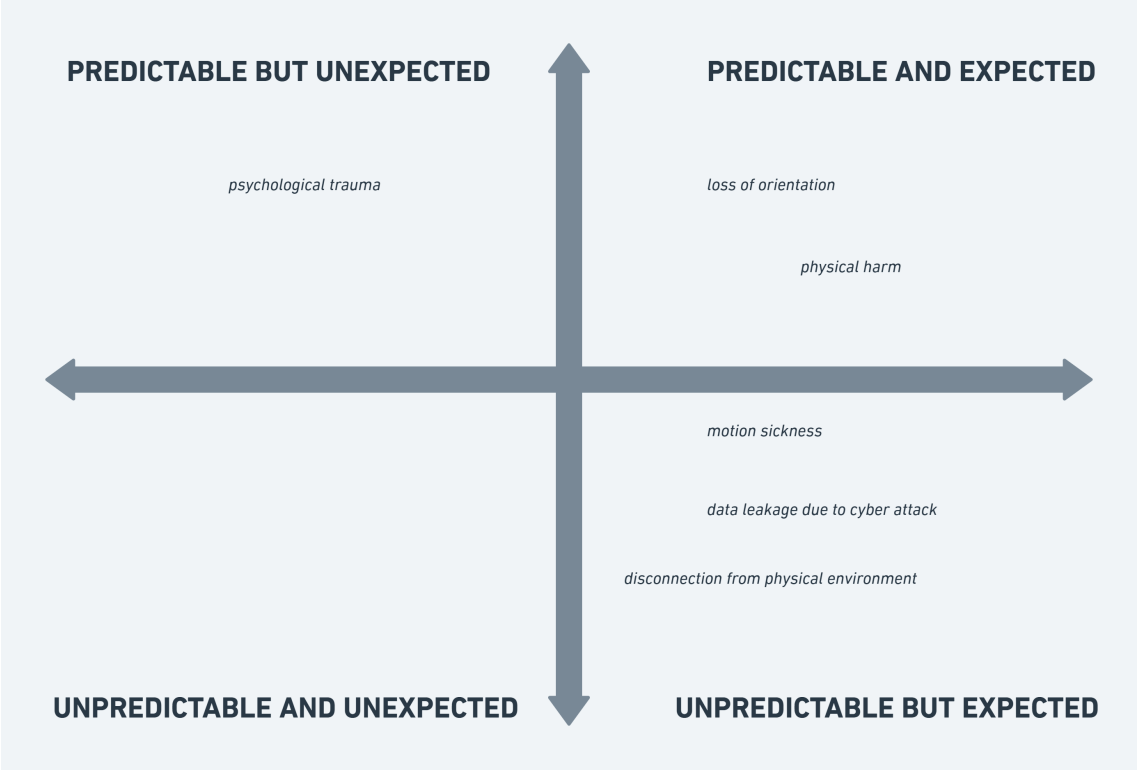

Figure 24. A Ellul-based model over possible ethical considerations "a priori"

The problems on which makes sense to focus in this framework are all but the unforeseeable and unpredictable problems. As a matter of fact, the thematic that most emerged from the interview is the impact on the user of known issues such as spacial limits and motion sickness which are problems that are known and thus (according to this model) they have ethical responsibility to address it. The same should be said about physical or psychological harm, which are problems that cannot

always be foreseen but that we can expect to happen at some point.

For these issues the following solutions are suggested:

7.1.1. Safe space

One of the major issues emerged in the survey questionnaire, was the inability of the users to be completely safe while in a virtual environment due to "bumping" and other incidents that can occur in the physical space around them. These guidelines can help create a space in which the users can constantly self-asses their own safety:

- Use in-software signals: step-counting, visual feedback and other signals can be used in-software to help the users remind to self-assess position in the physical space
- Use a mat: the use of recognizable surfaces (such as mats) or non rigid boundaries (such as tapes) are technique that can easily help the user identify a safe space while keeping the experience immersive;
- Proximity sensors: integrating proximity sensors with the other devices worn by users is an extra security measure; although it requires integration with the designed VR/AR environment it relief the users from having to check the surrounding environment during the experience
- Design a safe by default environment: not keeping objects at head or arm height creates an environment foolproof by design. In case of sit experience or standing experience in limited space, testing the area for sudden movements or violent reactions is an extra measure that can reduce the damage caused to users and structure
- Protect equipment: should everything else fail, putting extra protection on the equipment in the structure would allow at least to save the equipment and would avoid side-damage caused to users by broken equipment and

7.1.2. Better experience

Another issue highlighted by a vast part of the users was motion sickness. In some cases even the fear for motion sickness was a issue presented. The following guidelines offer a few remedies that should be implemented both in physical and virtual ambient to improve the user experience:

- Let user be in control: T1, B1 and B2 remarked the importance of not having the user feel lack of control over his/her experience. In order to achieve that the involuntary movements (movements that are not immediate consequence of a player's change of posture) should be eliminated, or reduced to minimum. Also, a smoother movement is not necessarily beneficial as it could trigger motion sickness (due to the fact that smoother movement are perceived as more realistic), thus developers should always keep in mind speed, direction, trigger and smoothness of the movement animation

- Allow refocus: refocusing refers to the action of re-orientating the camera to a preset perspective (foe example head height). In some videogames, the camera can be reset at any moment by pressing a button on the joypad, allowing the user to always access the most natural point of view during the experience. Implementing this feature in VR applications would give the user one more control tool over the experience and ensure that at any moment users are having a comfortable point of view

- Create a pleasant environment: Koch as demonstrated [91] that using pleasant odors and relaxing music effectively reduce the impact of motion sickness on users in a virtual environment

- Implement training sessions: from the questionnaire emerged that users believing in the necessity of change are wiling to make an extra effort; however if a user does not feel this incentive, making him/her aware of the fact that motion sickness can be overcome with training can provide a positive input. Making the users aware of the fact that they can overcome this issue and offering them the opportunity to get acquainted with virtual reality with less immersive experience is an effective incentive. T1 and B1 also confirm that some elements, like different degrees of field of view (figure 25), can help all the users enter VR/AR experience at their own pace.

Figure 25. An example of reduced field of view, source: https://newatlas.com/columbia-university-vr-motion-sickness/43855/

7.1.3. Other suggestions

More problems emerged between literature review, questionnaire and interviews. A few more guidelines that can improve VR/AR experience, independently from scope or audience, are the followings:

- Hygiene: given the necessity of physical movement, it is normal to assume that sweating and similar phenomena occur during a normal VR/AR experience. Especially for those that give access to the same headsets multiple times in a short time window, keeping spare parts, using cleaning wipes or using sterilizing box is necessary in order to guarantee a safe hygienic experience.
- Keep first-aid at hand: should any of the previous solutions fail, aggravation of physical harm can be mended in most situation by having at hand first-aid kits. It also contributes to keep hygiene of the experience as some users might present unknowingly scars or other conditions even before the VR/AR experience occurs

- Responsible data collection: as C1 mentioned, the best way to secure data is to not collect data. Only data that are relevant for the user experience or the core business should be collected, other sensible data (names, addresses, phone numbers) should not be kept unless necessary. Responsibility over data collection also consists of carefully selecting the resource allocation, as B3 stated: "all companies collect data that is critical and data that is not; not everything should be secure the same way, is important to allocate most of the resources to protect the information that has value"
- Ask feedback, prepare for being adaptive: as VR/AR evolves so should the developers. The survey showed that the users see the lack of communication between them and the developers as a barrier. Asking feedback and doing research on it is important to make the users cared for and to assess were the development community stands in their regards.

7.2. *A posteriori* solution

Let's now assume that all the candidates followed the best ethical code they knew and still something unethical happened. How would they assess themselves, how would they grow?

For this purpose, in this section is given a model that works in retrospective and offers an ever more tackling challenge on the moral issues. If we were to hypothetically turn into reality the considerations that all my interviewees had and then take them to the extreme point of execution we would see that the four main thematic that emerged (based on the following model) all of them would be acting unethically for more than one reason

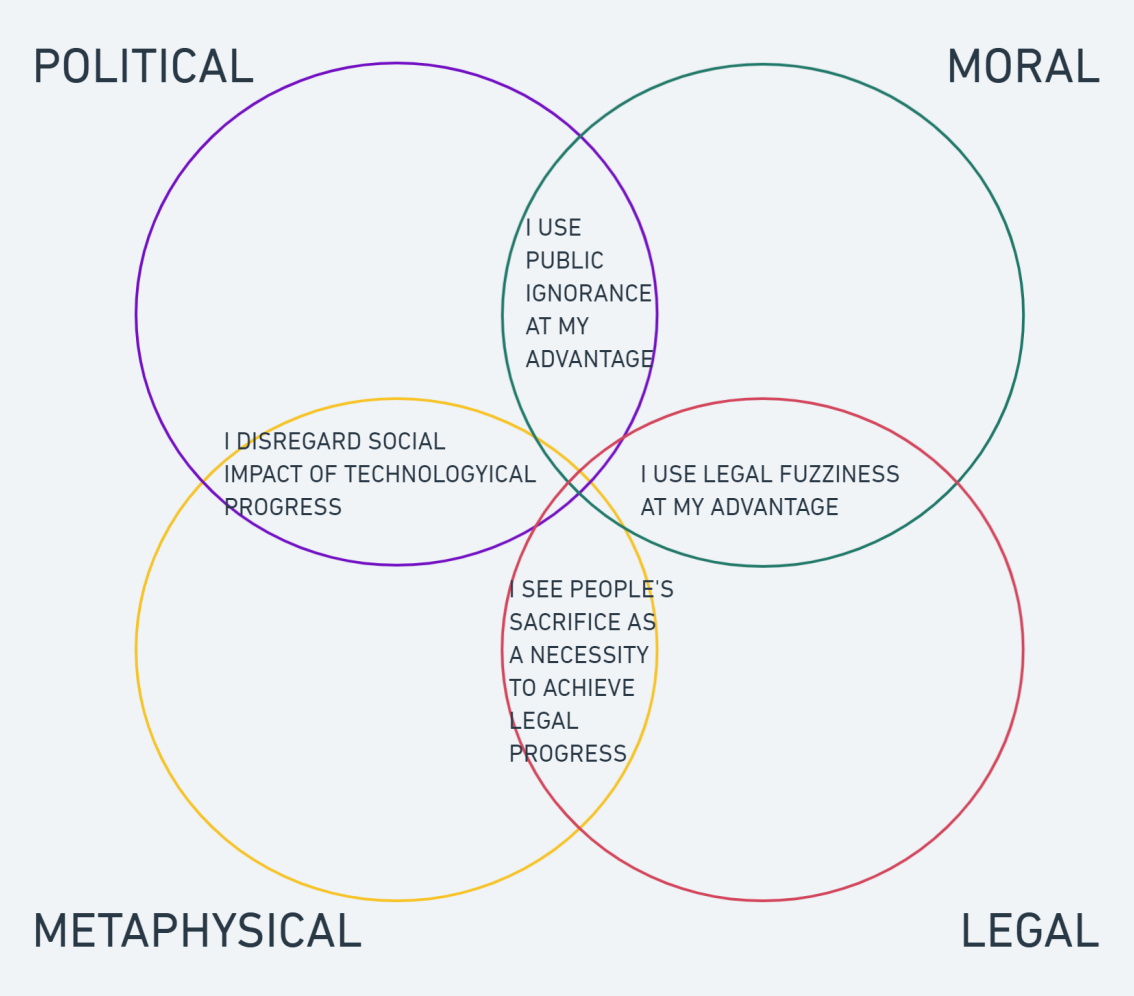

Figure 26. An ethical model based on Jaspers philosophy over the ethical question [1]

As can be noted, the model has been molded over the consideration made in the previous section and based on the ethical questions posed by Jaspers [83]. This way, a broader array of sensibilities and considerations can be explored, as the model is designed to work in non-exclusive connection, thus making it adaptable in different context.

For clarity, with this model the intention is not to imply that the interviewed candidates are culpable or guilty of any crime. The objective of this representation is to offer an easy graphical comparison of ideological conflicts that emerged during the interview and that can serve as well to others to question their own decision. It is my belief that the value of such model resides in the questions it spurs rather than the answers it provides.

In fact, in my case at least, the results of this model are very much conflicting with the ones discussed by the first model, where only one of the candidates would have had to re-assess his own ethical standards.

8. Conclusion

The presented research questions were:

1. Whether a person can be positively and uniquely identified based on recorded motion and single-channel EEG data?
2. Assuming this data is sensitive, how to securely collect, transmit and store it?
3. Explore data ethics considerations in this research, how can the modern ethical frameworks improve?

The first question was cleared through literature review. It is possible to identify and individual through recorded motion and EEG data; there are also additional PII that VR/AR devices collect, such as:

- Throw pattern
- Head-tilt
- Gaze tracking
- Hand movement

Moreover, this information, when combined with other data, still preserves the quality of PII.

The second question was cleared through literature research and interview with experts. A guideline has been provided complete with steps to be taken in order to securely transmit data in accordance with the law and in respect of the right to privacy of the users. Additional information and guidelines regarding security framework and policies have been lined out and their feasibility has been tested in a real environment. Interviews with the experts also offered a broader view on alternatives that are currently being adopted by business developers, technical developers and cybersecurity experts in the industry.

Finally the last question was cleared through interviews with experts and the survey questionnaire sent to the users. A variety of problems has been highlighted and to

these problems a solution was offered either by the experts who already are dealing with these issues or through research and experimentation in laboratory. To some ethical questions, such as the matter of responsibility, an answer was given in the form of guideline rather than a best practice, as some issues that emerged were to big to be effectively dealt with by the experts.

The most notable contributions of this dissertation are:

1. Data privacy and cybersecurity best-practice for small professional/research environments with VR/AR technologies
2. Ethical best-practice for the most common experience and ethical issues that emerge for the user in VR/AR experience
3. Cybersecurity and ethical guideline to follow in order to improve and expand the given guidelines
4. Survey of users opinions over VR/AR revealing the present opinion over security and privacy
5. Survey of experts revealing the present solution over security and privacy and problems in ethics

All these contributions have to be considered in light of the already highlighted limitations of the study, which are:

- The research and test on VR/AR products was made prevailing with reference to HTC Vive and Oculus Rift (which can impact the validity of contributions 1 and 3)
- The interviewees and survey participants were taken mainly from European countries and were discriminated based on their knowledge of VR/AR products (which can impact the validity of contributions 2, 3 and 4)
- The main cyber-attack vectors considered were data spoofing and impersonation (which can impact the validity of contribution 1)

Aside these limitations, a lot of improvements on the work done can be made, a few of which will be presented in the next section. The VR/AR technological landscape, as

expressed in the beginning, will all converge in that experience that is already being called by some XR. In this transition are virtually limitless the recommendations for research that should be done as the changes make new challenges emerge on a daily basis.

The development of this dissertation has indeed demonstrated that "our ability to develop technology is far superior to our ability to understand its consequences" [12]. This emerged not only during the interviews but also in the questionnaire, when the candidates shown that their desire for spreading of VR/AR devices was independent from the inability of the surveyed individuals to fully understand the technology they had at hand. From the same questionnaire we saw that people are taking for granted that some of their information are no longer secret when using most devices, thus reinforcing the assertion that "using technology transforms us" [12]. In such a context "the objection that technology is good or bad according to the use we make of it is no longer valid, because what modifies us is not whether it is used well or badly but the very fact that we use it at all" [12]. This consideration voids the argument opposed by most of the experts interviewed that still struggle to consider themselves fully accountable and responsible for all the consequences of the technology they contribute to develop and spread. As B2 argued "technology should be the solution, not the problem", but is not just the industry experts' but also the individuals' ability to contribute to the devising of a solution that seems to be strongly limited by the information asymmetry and the lack of relevant previous experience that can help foresee the consequence of our own actions.

The powerful impact that VR/AR devices will have is going to reshape the world; concepts like society, time and space are about to be completely revised.

Will the cybersecurity experts be in charge of finding the aforementioned "ἐπιστήμη", keeping technological revolution in balance with social development?

If so, may this dissertation be the first slab on the path.

8.1. Recommendations

On the cybersecurity side, the main problem is that SA in present time is far from the desired level [19]. For this reason Liu et al. [19] have devised a list of key capabilities that a cybersecurity team needs to develop in order to solve uncertain situations.

1. The ability to create problem-solving workflows or processes
2. The ability to see the big picture of cyber defense landscape
3. The ability to manage uncertainty
4. The ability to reason albeit incomplete/noisy knowledge
5. The ability to quickly locate needles in haystacks
6. The ability to do strategic planning
7. The ability to predict the possible next steps an adversary might take" [19]

In this thesis, a solution was offered in particular regarding point number 1,3,4 and 6. However, much more can be done to develop a model that would encompass all these key skills into a cybersecurity model that can manage uncertain situation and adapt itself to emerging threats.

Also on the technical side, a better guideline could be devised in light of the newly implemented support for TLS connection over Unreal Engine 4 version 4.24 [92].

For what concerns the user experience, future research should compound a list of visually, sound aiding/disrupting effects for developers to keep at hand; a problem emerged from the interviews as well as the questionnaire is the fact that some images and sounds are more likely than others to create distress/unease. In this dissertation, general guidelines were provided without specific reference to a particular type of sound or image. Such a deepening would probably require by itself a dissertation, for this reason it was not developed in this work; nonetheless there is evidence that such work would be appreciated by industry expert and would help clear the landscape over the element that negatively impact the UX.

On the ethics side, the framework presented can be improved, but what is most important is that these ethical considerations must be implemented in the legal landscape, as the next meaningful step of recognizing a social problem would be updating the legal landscape. Translating the ethical principle into a legal one would be the most effective way to deter the incurring of unethical behavior. On the same topic, more research could be done especially in regards of modern, emerging, philosophical consideration, as this dissertation took into account the work developed by exponents of philosophical currents up to the 20th century.

In general all the guidelines and the best practices presented could be improved in order to be applicable to more complex, even international, environments; the ethical considerations, on the other side, could greatly benefit from the opinion and experience of people coming from different cultures; interesting results would come out from confronting the opinions (especially in live sessions) of experts with differing not only on the professional background, but also on the cultural and social ones. The deeper the difference the more meaningful the validity of the defined "greater good".

References

[1] P. Rajivan and N. Cooke, "Impact of team collaboration on cybersecurity situational awareness," *Lecture Notes in Computer Science*, 2017.

[2] J. Reed, "Physical servers vs virtual machines: key differences and similarities," Dec. 2018. [Online]. Available: https://www.nakivo.com/blog/physical-servers-vs-virtual-machines-key-differences-similarities/

[3] C. Zhong, J. Yen, P. Liu, R. F. Erbacher, C. Garneau, and C. Bo, "Studying analysts' data triage operations in cyber defense situational analysis," 2017.

[4] Bloomberg, "Virtual reality market growing at a cagr of 33.47 percent and expected to reach 44.7 billion by 2024, exclusive report by marketsandmarkets," Online, 2019, https://www.bloomberg.com/press-releases/2019-07-05/virtual-reality-market-growing-at-a-cagr-of-33-47-and-expected-to-reach-44-7-billion-by-2024-exclusive-report-by.

[5] J. Dalton and J. Gillham, "Seeing is believing, how virtual reality and augmented reality are transforming business and the economy," PWC, techreport, 2019.

[6] Persistence Market Search, "Global market study on smartphones: android os to account for 50.7https://www.persistencemarketresearch.com/market-research/smartphones-market.asp

[7] MarketWatch, "Automotive market 2019 global industry share, size, revenue, latest trends, business boosting strategies, cagr status, growth opportunities and forecast 2024 - market reports world," Online, 2019, https://www.marketwatch.com/press-release/automotive-market-2019-global-industry-share-size-revenue-latest-trends-business-boosting-strategies-cagr-status-growth-opportunities-and-forecast-2024—market-reports-world-2019-07-01.

[8] J. Jerald, *The vr book, human-centered design for virtual reality*, M. T. Ozsu, Ed. ACM Books, 2016.

[9] M. F. Alam, S. Katsikas, O. Beltramello, and S. Hadjiefthymiades, "Augmented and virtual reality based monitoring and safety system: a prototype iot platform," *Journal of Network and Computer Applications*, vol. 89, 2017.

[10] R. Chatwood, “Virtual legality virtual reality and augmented reality, legal issues,” Dentons, Tech. Rep., 2017.

[11] J. C. Wong, “Sexual harassment in virtual reality feels all to real, "it’s creepy beyond creepy",” Oct. 2016. [Online]. Available: https://www.theguardian.com/technology/2016/oct/26/virtual-reality-sexual-harassment-online-groping-quivr

[12] U. Galimberti, “Man in the age of technology,” *Journal of Analytical Psychology*, vol. 54, pp. 3,17, 2009.

[13] B. Kenwright. (2019, Jan.) Virtual reality: ethical challenges and dangers. [Online]. Available: https://technologyandsociety.org/virtual-reality-ethical-challenges-and-dangers/

[14] E. Craig and M. Georgieva, “Vr and ar: the ethical challenges ahead,” Apr. 2018. [Online]. Available: https://er.educause.edu/blogs/2018/4/vr-and-ar-the-ethical-challenges-ahead

[15] D. Adams, A. Bah, C. Barwulor, N. Musaby, K. Pitkin, and E. M. Redmiles, “Ethics emerging: the story of privacy and security perceptions in virtual reality,” in *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 427–442. [Online]. Available: https://www.usenix.org/conference/soups2018/presentation/adams

[16] T. P. Jung, “Introduction to electroencephalogram,” Department of Computer Science, National Chiao-Tung University.

[17] B. C. Armstrong, M. V. Ruiz-Blondet, N. Khalifian, K. J. Kurtz, Z. Jin, and S. Laszlo, “Brainprint: assessing the uniqueness, collectability, and permanenceof a novel method for erp biometrics,” May 2015.

[18] D. L. Dimitrios Zissis, “Addressing cloud computing security issues,” *Future Generation Computer Systems*, vol. 28, pp. 583–592, 2012.

[19] P. Liu, S. Jajodia, and C. Wang, *Theory and models for cyber situation awareness*, G. Goos, J. Hartmanis, and J. van Leeuwen, Eds. Springer, 2017.

[20] A. Kupin, B. Moeller, Y. Jiang, N. K. Banerjee, and S. Banerjee, “Task-driven biometric authentication of users in virtual reality (VR) environments,” in *International conference on multimedia modeling*, 2018.

[21] J. A. de Guzman, K. Thilakarathna, and A. Seneviratne, "Security and privacy approaches in mixed reality: a literature survey," *ACM Comput. Surv*, vol. 52, no. 6, 2018.

[22] S. Morgan, "2019 official annual cybercrime report," 2019.

[23] D. Q. Ekaterina R. Stepanova and B. E. Riecke, "Space, a virtual frontier: how to design and evaluate a virtual reality experience of the overview effect," *Frontiers in digital humanities*, Apr. 2019. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fdigh.2019.00007/full#F2

[24] Bain&Company, "Augmented reality," Oct. 2018. [Online]. Available: https://www.bain.com/insights/customer-experience-tools-augmented-reality/

[25] "Steam hardware-software survey," Nov. 2019. [Online]. Available: https://store.steampowered.com/hwsurvey/Steam-Hardware-Software-Survey-Welcome-to-Steam

[26] W. Fenlon, "Steam now has 90 million monthly users," Jan. 2019. [Online]. Available: https://www.pcgamer.com/steam-now-has-90-million-monthly-users/

[27] L. Lanier, "Steam now has one billion accounts (and 90 million active users)," Apr. 2019. [Online]. Available: https://variety.com/2019/gaming/news/steam-one-billion-accounts-1203201159/

[28] K. Pfeuffer, Ed., *Behavioural biometrics in vr: identifying people from body motion and relations in virtual reality*, May 2019.

[29] A. Z. Majed, S. Tregillus, and E. Folmer, "Handsfree omnidirectional vr navigation using head tilt," Aug. 2017. [Online]. Available: https://www.researchgate.net/publication/311575574_Handsfree_Omnidirectional_VR_Navigation_using_Head_Tilt

[30] Y. Yan, Y. Chun, X. Yi, and S. Yuanchun, "Headgesture: hands-free input approach leveraging head movements for hmd devices," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 4, 2018. [Online]. Available: http://pi.cs.tsinghua.edu.cn/lab/papers/headgesture_Hands-Free%20Input%20Approach%20Leveraging%20Head%20Movements%20for%20HMD%20Devices.pdf

[31] J. Lee, S. C. Ahn, and J.-I. Hwang, "A walking-in-place method for virtual reality using position and orientation tracking," *MDPI*, 2018. [Online]. Available: http://www.mdpi.com/1424-8220/18/9/2832/pdf-vor

[32] V. Mohan, "Better biometrics in andoid P," Jun. 2018. [Online]. Available: https://android-developers.googleblog.com/2018/06/better-biometrics-in-android-p.html

[33] C. Brubaker, "Changes to trusted certificate authorities in android nougat," Jul. 2016. [Online]. Available: https://android-developers.googleblog.com/2016/07/changes-to-trusted-certificate.html

[34] P. Sharma, "Fingerprint sensor is becoming standard feature in smartphones," Online, Sep. 2017. [Online]. Available: https://www.counterpointresearch.com/fingerprint-sensor-is-becoming-standard-feature-in-smartphones/

[35] Apple Official Website, "About face id advanced technology," Oct. 2019. [Online]. Available: https://support.apple.com/en-gb/ht208108

[36] A. Tepljakov, "Re:creation." [Online]. Available: Https://recreation.ee/

[37] F. Z. Qureshi, "Object-video streams for preserving privacy in video surveillance," *Advanced Video and Signal Based Surveillance*, 2009.

[38] B. E. Deborah D. Deborah, M. Ann Reinthal and G. Goodman, "Privacy-Aware Human Motion Tracking with Realtime Haptic Feedback," *2015 IEEE International Conference on Mobile Services*, 2015.

[39] F. Roesner, T. Kohno, and D. Molnar, "security and privacy for augmented reality systems," *Communications of the ACM*, 2014.

[40] Y. A. Sekhavat, "Privacy preserving cloth try-on using mobile augmented reality," *Leee transactions on multimedia*, vol. 19, no. 5, pp. 1041,1049, May 2017.

[41] L. W. Benjamin C.M. Fung, Ke Wang and P. C. K. Hung, "privacy-preserving data publishing for cluster analysis," *Data Knowledge Engineering*, 2009.

[42] M. T. Yang Xu, Tinghuai Ma and W. Tian, "a survey of privacy preserving data publishing using generalization and suppression," *Applied Mathematics & Information Sciences*, 2014.

[43] Aristotelis, "The Nicomachean ethics."

[44] S. Persky, Jessica Outlaw, "Industry review boards are needed to protect VR user privacy," Aug. 2019. [Online]. Available: https://www.weforum.org/agenda/2019/08/the-hidden-risk-of-virtual-reality-and-what-to-do-about-it/

[45] H. Chung, M. Iorca, j. Voas, and S. Lee, "Alexa, can i trust you?" *Computer (NIST)*, 2017.

[46] A. Graham and R. Hagarty, "Build a virtual assistant that responds to a trigger word," Apr. 2019. [Online]. Available: https://developer.ibm.com/tutorials/add-a-trigger-word-to-your-watson-assistant/

[47] R. Khanna, "Rep. Ro Khanna at the 2019 Web Summit in conversation with Brad Smith, Microsoft CEO," Online, Nov. 2019. [Online]. Available: https://www.youtube.com/watch?v=azv9glrrrco

[48] Cspan, "Facebook CEO Mark Zuckerberg hearing on pata privacy and protection," Apr. 2018. [Online]. Available: https://www.c-span.org/video/?443543-1/facebook-ceo-mark-zuckerberg-testifies-data-protection%20Accessed%204/15/18

[49] A. Perrin, "Many US Facebook users have changed privacy settings or taken a break," Online, Sep. 2018. [Online]. Available: https://students.mathsnz.com/3.12/pdfs/Article15.pdf

[50] C. De Froidmont, L. Donati, M. Steffen, and A. Zaidi, "China's social credit system - analysis of a socio-technical controversy," Apr. 2018, https://mastertsinghua.wordpress.com/2018/04/30/chinas-social-credit-system-analysis-of-a-socio-technical-controversy-by-cassandre-de-froidmont-ludovica-donati-miriam-steffen-and-aiman-zaidi/.

[51] Central Government of China, "State council on printing and distributing social credit system notice of planning outline (2014-2020)," Online, 2019. [Online]. Available: http://www.gov.cn/zhengce/content/2014-06/27/content8913.htm

[52] S. Mistreanu, "Life inside China's social credit laboratory," Online, Apr. 2018. [Online]. Available: https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/

[53] N. Doorn and I. van de Poel, "Editors' overview: moral responsibility in technology and engineering," Jun. 2011. [Online]. Available: https://link.springer.com/content/pdf/10.1007%2fs11948-011-9285-z.pdf

[54] K. S. Young, "What makes the internet addictive: potential explanations for pathological internet use," American Psychological Association, Aug. 1997.

[55] C. S. Culbertson, S. Shulenberger, R. de la Garza, T. F. Newton, and A. L. Brody, "Virtual reality cue exposure therapy for the treatment of tobacco dependence," *PubMed Central*, 2012. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4204479/

[56] M. A. Lemley and E. Volokh, "Law, virtual reality, and augmented reality," *University of pennsylvania law review*, vol. 166, no. 5, Apr. 2018.

[57] N. Kshetri, "The simple economics of cybercrime," *IEEE Security and Privacy Magazine*, 2006. [Online]. Available: https://www.researchgate.net/publication/3437766_The_simple_economics_of_cybercrimes

[58] "IEEE xplore webiste," 2019, retreived on 19/08/2019. [Online]. Available: https://ieeexplore.ieee.org/Xplore/home.jsp

[59] "Google scholar," 2019. [Online]. Available: https://scholar.google.com/

[60] "Researchgate," 2019. [Online]. Available: https://www.researchgate.net/

[61] "ScienceDirect," 2019. [Online]. Available: https://www.researchgate.net/

[62] E. Gasten, Thomas and B. H. Smith, *The research paper: a commonsense approach.* Englewood Cliffs: Prentice Hall, 1988. [Online]. Available: https://jeaune.public.iastate.edu/Horticulture_LC_105/Web/Determiningauthoritativesource.htm

[63] Solid It, "System properties comparison influxdb vs. mysql vs. prometheus," 2019. [Online]. Available: https://db-engines.com/en/system/InfluxDB%3BMySQL%3BPrometheus

[64] Y. W. Bernier, "Latency compensating methods in client/server in-game protocol design and optimization," 2017. [Online]. Available: https://www.gamedevs.org/uploads/latency-compensation-in-client-server-protocols.pdf

[65] K. Raaen and T. M. Gronli, "Latency thresholds for usability in games: a survey," Oct. 2014.

[66] M. L. Chenechal and J. Chatel Goldman, "HTC Vive Pro time performance benchmark for scientific research," Nov. 2018.

[67] T. Sweeney, "Unreal Engine 4," 2014. [Online]. Available: https://www.unrealengine.com/en-us/

[68] EDPB Plenary Meeting, *Guidelines 4/2019 on article 25 data protection by design and by default*, Nov. 2019.

[69] Parliament of European Union, "Regulation (eu) 2016/679 of the european parliament and of the council (General Data Protection Regulation)," 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679

[70] B. Wolford, "Data processing agreement (template)," 2019. [Online]. Available: https://gdpr.eu/data-processing-agreement

[71] R. Dewri, I. Ray, I. Ray, and D. Whitley, "On the optimal selection of k in the k-anonymity problem," IEEE 24th International Conference on Data Engineering, Apr. 2008.

[72] K. E. Emam and F. K. Dankar, "Protecting privacy using k-anonymity," Journal of the American Medical Informatics Assosiaction, Sep. 2008.

[73] V. S. Verykios, E. Bertino, I. N. Fovino, L. P. Provenza, Y. Saygin, and Y. Theodoridis, "state-of-the-art in privacy preserving data mining," *ACM SIGMOD Record*, 2004.

[74] World Bank and United Nations, *Combatting cybercrime: tools and capacity building for emerging economies*, Washington DC: World Bank, Ed. The world bank IBR IDA Group, 2017. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/worldbank-combating-cybercrime-toolkit.pdf

[75] E. J. Chesney, "Concept of mens rea in the criminal law," *Journal of Criminal Law and Criminology*, vol. 29, Jan. 1939. [Online]. Available: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=2828&context=jclc

[76] D. Lanius, *Strategic indeterminacy in the law.* Oxford university press, May 2019.

[77] Legal Information Institute Cornell Law School, "Mens Rea," Online Library, 1992. [Online]. Available: https://www.law.cornell.edu/wex/mens_rea

[78] J. Gardner, "The negligence standard: political not metaphysical," *Modern Law review*, 2017. [Online]. Available: https://johngardnerathome.info/pdfs/negligencestandard.pdf

[79] D. Baumgold, "Hobbes's and Locke's contract theories: political not metaphysical," *Critical Review of International Social and Political Philosophy*, vol. 8, no. 30, Sep. 2015.

[80] M. Heidegger, *The question concerning technology.* Garland publishing, 1954.

[81] L. Carriero, "Dire la verita: parresia," *La Stampa*, Apr. 2012. [Online]. Available: https://web.archive.org/web/20130104221424/http://www.lastampa.it/2012/04/22/blogs/la-bussola-d-oro/dire-la-verita-parresia-TOuZItx9tJaHOQtrpPrxrO/pagina.html

[82] M. Weber, "Politics as vocation," 1919.

[83] K. Jaspers, *The question of the german guilt.* Britannica, 1947.

[84] G. Molina, M. Musy, and M. Lefranc, *Building professionals facing the energy efficiency challenge.* Wiley, 2018.

[85] I. Kant, "Groundwork of the Metaphisics of Morals," 1785.

[86] C. Zimmerman, *Cybersecurity operations center.* The MITRE Corporation, 2014. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

[87] N. J. J. Smith, *Vagueness and degrees of truth.* Oxford University Press, 2008.

[88] Epic Games, "Unreal Engine 4," 2012. [Online]. Available: https://www.unrealengine.com/en-us/

[89] *Routine and non-routine problem solving*, ser. Mathematical Tale Winds. Winnipeg. MB. Canada: Faculty of Education, University of Winnipeg, Mar. 2012.

[90] ENISA, "Zero-day," 2016. [Online]. Available: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/zero-day

[91] A. Koch, I. Cascorbi, M. Westhofen, M. Dafotakis, and S. Klapa, "The neurophysiology and treatment of motion sickness," Oct. 2018. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6241144/#R36

[92] Epic Games, "Unreal Engine 4.24 release notes," 2019. [Online]. Available: https://docs.unrealengine.com/en-US/Support/Builds/ReleaseNotes/4_24/index.html