THE ROLE OF AI IN PREVENTION THE SPREAD OF SPORTS ILLEGAL STREAMING SERVICES IN DENMARK

MASTERTHESIS
to obtain the Erasmus Mundus Joint Master Degree

by Digital Communication Leadership (DCLead)

of
Faculty of Cultural and Social Sciences
Paris Lodron University of Salzburg

Technical Faculty of IT and Design
Aalborg University in Copenhagen

Submitted by
AIGERIM BAIGUNUSSOVA
Student number at PLUS s1061298
abaigu19@student.aau.dk
Vognporten 14-237, Albertslund, 2620, Denmark

Primary Supervisor: Anders Henten
Secondary Supervisor: Tales Tomaz

Department of Communication Studies

Salzburg, 15.11.2020

Table of content

Table of figures and tables

Executive Summary

This research looked at the use of illegal sports streaming services in Denmark, as well as methods of dealing with them. In particular, the researcher focused on AI technology as a solution that, in combination with other forces, is able to counter the proliferation of sports streaming in Denmark.

Research question:

What is the role of AI in the battle against illegal sports streaming services ?

Sub questions:

What factors are driving the use of AI in the fight against sports piracy?

What additional forces in combination with AI influence this fight?

The author applied The TOE model and The Pathetic Dot Theory of Lessig to create a theoretical framework, which further helped to analyze empirical data. The research is qualitative and the method of collecting empirical data was semi-structured interviews, which were conducted with representatives from The Danish Rights Alliance and Irdeto company, which is developing an AI solution to combat sports streaming piracy. During the analysis of the collected data, the author identified factors influencing the use of AI, as well as what other movers are able to support this battle. As the author found out, in the chain of activities against piracy, AI plays one of the crucial roles, but also, the existence of factors affecting the end-user is also significant and can make a huge contribution to the process of reducing piracy of sports content in Denmark.

Introduction

1.Background

At the beginning of the thesis, the author decided to provide the reader with information about the situation in Denmark regarding the use of illegal streaming services, since the research topic focuses on them as the main tool for accessing pirated broadcast sports events. Next, the researcher explained the most common methods of streaming services and their monetization process, which is based on promoting advertising on these websites. This chapter concludes by presenting data on the reasons for the attractiveness of the abovementioned services.

The author hoped that after reading this chapter, it will be easier for the reader to understand the principles of operation and the reasons for the emergence of illegal streaming services, which will reveal the full picture of the author's motivation, that prompted her to choose the topic of this work.

1.1 Situation in Denmark

According to a study by the Danish Rights Alliance (2018), an anti-piracy group representing local and international rightsholders, danes visited 2,000 leading pirate sites 596 million times, the traffic to pirate sites increased 67% between 2016 and 2017. The Rights Alliance claims that Denmark has one of the most effective blocking systems in the world, but it still does not stop a huge number of people from consuming pirated content. (Rights Alliance,2019)

Illegal live sports services have also captured the interest of the Danes. In 2017 alone, Danish IP addresses visited pirated sites with live streaming of sports matches 2.96 million times, which is almost 250,000 monthly visits. From January to December 2017, the Rights Alliance recorded a 28 percent increase. Unlike the Internet Protocol television (IPTV) pages, the numbers more closely reflect the actual consumption, since

it is necessary to visit the illegal site every time you want to watch a match. In addition, there is also an indication that users have found 'favorite services', as over half of the traffic to the pages comes from direct entries and not through searches with, for example, Google's search engine. (Rights Alliance,2019)

In Divisionsforeningen, Klaus Thomsen called illegal broadcasting a serious problem because it threatens club revenue from television broadcasts and commercials. “The consequences for Danish football, in the end, may be that the revenue base will be less, and then we will play the worst football”, he says. (Nybom, Skov-Jensen, 2018)

“In the extreme, it may be that the TV stations no longer want to make TV deals with the clubs if their viewership drops, because people can watch it for free on the internet around them. TV-money is very important. Without it we would not be able to have the same squad that we know today”, says Jacob Juul Jørgensen (Nybom, Skov-Jensen, 2018).

In order to understand how easy it is to connect to illegal services that broadcast sports events, there is a need to provide an explanation of these services, which are called Peer-to-peer live streaming and Free live streaming services.

1.2 Approaches for illegal live content delivering

According to Leporini (2017), there are two main ways of delivering illegal live content. The first approach is Peer-to-peer live streaming and the second is Free live streaming services.

1.2.1 Peer-to-peer (P2P) live streaming

The history of P2P technology originates from Napster in 1999, when users used “their” bandwidth to exchange primarily musical content. This happened long before the CDN, which in the modern world has become the standard means for sharing content (Leporini, 2017).

As it stated by Leporini (2017), in the distant 2000s, the Chinese P2PTV protocols (e.g., PPLive or PPStream) began to exchange content. The idea of sharing was based on limiting the bandwidth of servers, which is not entirely clear. In most cases, these protocols are derived from real-time-enabled BitTorrent, which with the development of technology are also evolving.

The principle of P2P streaming is explained by Leporini (2017), "P2P users sharing the same content form a loosely connected mesh network compared with a full mesh network where all peers are connected to all other peers." This ensures reliability and stability of the P2P network because stopping one network node does not affect the operation of the remaining nodes, they can reconnect if necessary (see Figure 1).

In an accessible language, all computers of a network are connected to each other which allows communication without the intervention of a third party (Kariyawasam and Tsai, 2017).

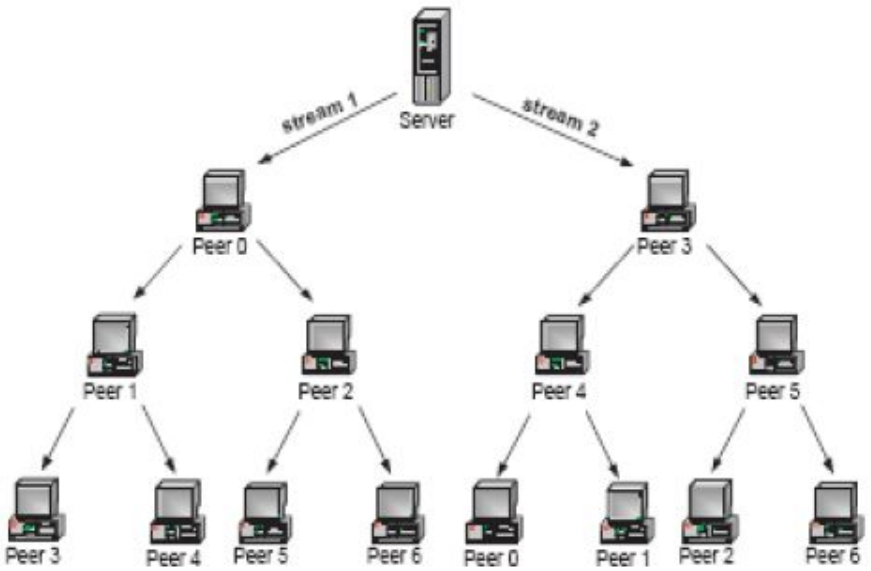

Figure 1. P2P network

As it was claimed by Kariyawasam and Tsai (2017), P2P technology has gained popularity among sport viewers since it provides the opportunity to consume online sport content without any intercommunications between participants of P2P sharing. The two main characteristics of P2P streaming play an influential role for sport content consumers. The first characteristic is "limitless", which is explained by the fact that the P2P network enables sending content to an enormous number of network participants, which is typical for P2P file sharing, therefore it is also common for live streaming P2P protocols. Leproni cited an example (2017), one of his measures over such P2P streaming networks resulted in 30,000 viewers per a specific stream on a regular basis. The second characteristic is the high quality of streams which is usually significantly higher in terms of achievable bitrate (the number of bits used to transmit / process data per unit time). As maintained by Leproni (2017): “Whereas the majority of direct Web streaming bitrates are lower than 600Kbps, our knowledge base shows that 60 percent of the P2P streams have bitrates below 2Mbps, 30 percent between 2Mbps and 4Mbps, and the remaining streams with bitrates above 4Mbps.”

On average, less than 10 percent of all direct illegal broadcasts account for P2P streaming, which is a fairly low rate compared to other types of streams. Moreover, tracking P2P streams is a rather complicated process, since P2P protocols are usually closed-source (Leproni, 2017).

1.2.2 Free live streaming services

In the early 90s, the Internet began to gain momentum, but despite this fact, the transmission of sound and video remained difficult until the year 95 of the last century, when online streaming technologies were introduced. The first online streaming baseball match between the New York Yankees and the Seattle Mariners was broadcast by Progressive Networks. In the modern world, online streaming occurs every second around the world (Rafique, Goethem, Joosen,Huygens, Nikiforakis, 2016).

According to Rafique, Goethem, Joosen,Huygens, Nikiforakis (2016), “This massive consumption and endorsement of online video brought with it the rise of extremely popular services for free live streaming (FLIS)”. FLIS are services that allow users to view video broadcasts for free, mainly without the consent of the content producer and television channels that conduct live broadcasts (Rafique, Goethem, Joosen,Huygens, Nikiforakis, 2016).

Rafique, Goethem, Joosen, Huygens, Nikiforikis conducted research on the infrastructure of these services based on 23,000 web pages. According to the study, approximately 64 percent of services at least once were found to be in violation of property rights. It is worth noting that the researchers focused on sports broadcasts, because basically this area is the most popular and prone to attacks, and producers of original content are more likely to report a violation of their rights to ownership. FLIS services locate their infrastructure primarily in Europe and Belize and are involved in non-standard advertising methods, possible trademark infringement and fraudulent activities aimed at its users, as well as television broadcasters and sports organizations (Rafique, Goethem, Joosen,Huygens, Nikiforakis, 2016).

According to Rafique, Goethem, Joosen,Huygens, Nikiforakis (2016), the FLIS ecosystem consists of three main parties: **channel providers, aggregators, and advertisers** (Figure1).

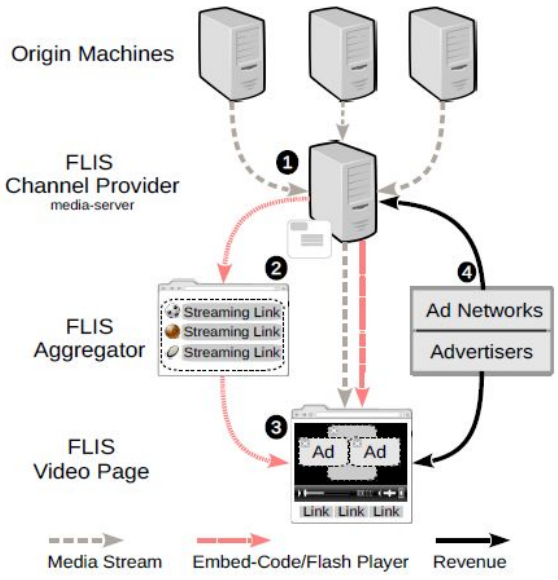

Figure 2. FLIS structure

Channel providers provide the infrastructure to promote online streaming. In particular, the channel provider supports a media server that can be used by any user for free. The purpose of the media server is to receive streaming video in real-time from a remote machine and broadcast it to a wide range of viewers on the Internet. The remote machine can be controlled by the channel provider itself or it can belong to another third-party provider.

Aggregators catalog codes for embedding streams, usually from different channel providers, and index links to various free live streams on their web page. In other words, they provide a free one-stop site for viewing many live events and TV channels.

Advertisers and ad networks are the primary source of revenue for all of the FLIS infrastructure. Channel providers and aggregators include JavaScript code from ad networks to monetize their operations. Ad network code downloads and displays ads from different advertisers on top of the Flash player. Every time when a user clicks on an ad advertisers will pay the ad network for the visitor, who, in turn, will pay the publisher

the channel provider or the aggregator based on the pre-negotiated payment model (Rafique, Goethem, Joosen,Huygens, Nikiforakis, 2016).

Another researchers Ayers and Hsiao (2019), from Stanford University, who also studied the nature of Free live streaming services illustrated the relationship of parties of FLIS. According to them, there are five main participants of FLIS (Figure 2): **media providers, channel providers, advertisers, aggregators, users.**

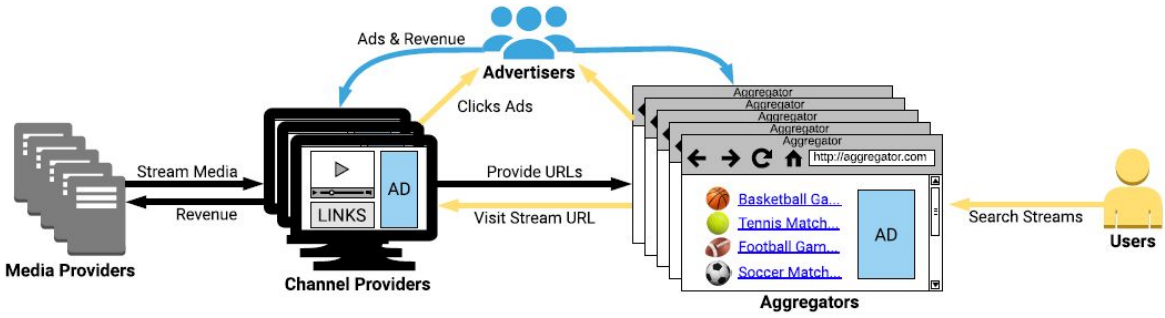

Figure 3. Relationship of parties of FLIS

Media providers are the owners of original stream content. A media provider may be a single individual streamer sending a video stream using software, or a large entity such as a broadcasting station. When it comes to illegal content streaming, a media provider could be an individual who subscribes to a paid service and rebroadcasts this content for free in real time.

Chanel providers receive content from media providers and host web-pages on which illegal streams can be watched. Youtube and Twitch are examples of legal channel providers. Examples of illegal services include sites like buffstreamz.com or watchsport.fun.

Aggregators gather links of various channel providers for making them available for discovering and browsing by users. Some of them provide a list of streams, others allow searching for specific content that is available at the moment. In some cases,

aggregators themselves may also serve as channel providers, such that when a user clicks on a link to a live event, they do not leave the aggregator domain.
According to Ayers and Hsiao (2019), **advertisers** as it was explained by Rafique, Goethem, Joosen,Huygens, Nikiforakis (2016), play the fundamental role in the infrastructure of FLIS and help to monetize the whole process of delivering illegal streaming content to users.
Users are those who consume illegal streaming content that is provided by channel providers and aggregators.

According to researchers Rafique, Goethem, Joosen, Huygens, Nikiforikis (2016), who collected information on 23,000 web pages that provide illegal access to sports broadcasts, these services use methods that can mislead users. Thus benefiting from a huge user database, streaming service primarily endangers end-user computers and their personal data. For example, the above websites use advertising methods that encourage users to click the fake buttons to close the advert overlay that appears while watching a sports stream. This technique can trick a user who naively clicks on a fake button, potentially exposing it to malicious websites (Rafique, Goethem, Joosen,Huygens, Nikiforakis, 2016). When it comes to harming the copyright holders of the original sports content, the damage can be counted in millions. As a result of illegal sports streaming services, owners of broadcasting rights, sports organizations and television channels suffer as they only have exclusive rights to any broadcast of their games on the Internet. Law enforcement authorities can detect and block any domain or IP address involved in the broadcast of illegal sports broadcasts, based on their territorial jurisdiction. Despite this, FLIS finds methods to continue its business and can hide behind third parties or located in places where laws are not very strong in combating them. In addition, FLIS parties often use certain territorial laws, claiming that they are not involved in direct copyright infringement. Aggregators state that they only index links to live broadcasts of sports, and channel providers claim that they act only as

providers of media servers that transmit streams to an unrelated third party (Rafique, Goethem, Joosen,Huygens, Nikiforakis, 2016).

1.3 Reasons for the attractiveness of illegal sports broadcasts

1.3.1 “Digital lemon” phenomenon

Broadcasting sports events can be attributed to the concept of “digital lemon”, as explained by Hoof (2016). According to Hoof, the phenomenon of “digital lemon” is quite suitable for sports broadcasting because these transmissions are live.

As it is stated by Chen (2020), “The lemons problem refers to issues that arise regarding the value of an investment or product due to asymmetric information possessed by the buyer and the seller”. In other words, the owner of the product or the one who provides the service has an idea of the value of the product/service or can evaluate its level above or below average. In turn, the one who purchases the product/service does not have the full information that the seller has about the product/service.

As it was explained by Hoof (2016), sports broadcasts are of great value, unlike music or films that can be downloaded to a computer. Sports broadcasts are relevant when users have access to live broadcasts and the ability to watch the game in parallel when it takes place at a football stadium or basketball court. At the end of the event, the game results are already known, and in most cases, users no longer show interest in a particular game. If we are talking about illegal broadcasts, the digital lemon phenomenon has a greater impact on them than on music or movies that are downloaded and stored on the user's computer.There are many reasons why an illegal broadcast of a sporting event may be interrupted. For example, due to a technological malfunction or the identification of copyright infringement.Thereby, users of illegal content have limited chances to switch to legal broadcasting.In this case, individuals face costs that are fundamentally different

from downloading music or films due to the non-reproducible liveness of sports events. This explains why live sports are valuable to content providers (Hoof, 2016).

1.3.2 “Easy to create and difficult to shut down”

Another reason why illegal sports streams are gaining popularity is that they are “easy to create and very difficult to close”. These websites pose a huge threat to copyright holders, as they encroach on the main property of television and radio broadcasters: live audio-visual broadcasts of a sporting event (Hoof, 2016). Providing users with access to a particular sporting event, regardless of the user's location, illegal sports websites are destructive, as they destroy the carefully organized geography of broadcast rights.It becomes obvious why the “media sports industry professionals" don’t really like websites with illegal content that are “easy to create and difficult to shut down”.
This is especially due to the fact that a lot of money is spinning in the world of sports. Every year, television companies spend millions on the acquisition of ownership of the broadcast of a major sporting event. Hoof gives several such examples. Fox Sports paid over $ 400 million in 2011 for rights to the 2018 and 2022 World Cups, while NBC paid $ 7.65 billion for the right to broadcast the Olympic Games from 2022 to 2032. These sums of money are so huge that sports clubs earn the bulk of their income from selling the rights to broadcast the event.
At the end of August 2017, at the Mayweather-McGregor historic battle, where the prize winners were at least $ 300 million, profit from broadcasts, tickets, and sales of merchandise was added to the guaranteed amount of 100 million. At the same time, about 100 million users watched this fight illegally, at that time making it the most pirated event in the history of sports (Kokorina,2017).
The fight could be watched legally (for 89.95 dollars in normal quality and for 99.95 - in HD) or for free: pirate streams constantly appeared on Facebook, Twitter, Instagram and YouTube. The satellite company Irdeto discovered 239 illegal broadcasts, 472 thousand

people connected to one of them simultaneously: only these viewers would have brought the organizers about $ 43 million (Kokorina,2017).
Hoof also noted that downloading streams of sports matches for online broadcasts is not difficult, since there are many online guides explaining this process (Hoof, 2016)

1.3.3 Lingua franca

In addition to the above, Hoof explained the high demand for illegal broadcasts by the fact that sport does not have to be broadcast in one or another language, as is the case with narrative broadcasts, where language has a key role. Thus, geoblocking circumvention allows the consumption of pirated broadcasts to be more flexible. According to Hoof (2016) "Much of the media accessed through circumvention is either diasporic in its nature, with expats often sourcing media content from their home country, or read through a particular form of Western hegemony (e.g. everyone trying to access U.S. Netflix). However, while there is still a Western bias present, sports fans are likely to engage in more transnational forms of consumption." Therefore, as stated by Hoof, sport can be perceived without any language restrictions and is a kind of lingua franca because of geoblocking circumvention practice. Thus, it becomes easier for inveterate sports fans to follow their favorite athletes or matches, for example, a football fan can easily watch the African Cup of Nations or an Australian tennis fan watch the Association of Tennis Professionals match in Swedish (Hoof, 2016).

1.3.4 Attraction for scammers

Most of the websites providing access to pirated sports broadcasts use the truthfulness and inexperience of users, which ultimately harms them. The advertising market in such websites is quite extensive. Operators use their services to promote advertising by displaying several ads through pop-ups or Flash content. Some of them steal personal

information, subsequently carry out fraudulent operations with user credit cards, or malicious programs spread that also pose a threat to individuals.Using fake plugins, updates, or installers of video player software; prepared hidden, transparent buttons are common on such websites. Operations with Javascript-based drive-by-download attacks; or using security holes in software such as Flash are examples of fraud. Consumers who rely on real-time illegal broadcasts significantly increase the risk of such attacks (Hoof, 2016).

In their research, Ayers and Hsiao (2019), claimed "These sites are by definition criminal enterprises but require substantial audiences in order to profit—as a result, they are easy to locate and make little attempt to hide from security researchers. These sites serve as an excellent case study of modern techniques used to profit off of users, whether that be via deceptive ads, abuse of affiliate programs, user tracking, or distributing malware."

2. Research questions

Based on the information described above, the author of this study intends to look at the current process of combating illegal sports streaming services in Denmark and how artificial intelligence can influence this process. Through subquestions, the researcher tries to discover the factors affecting the application of AI in the sports broadcasting industry, as well as consider other measures to prevent streaming sports piracy.

Main Question:

What is the role of AI in the battle against illegal sports streaming services ?

Sub Questions:

What factors are driving the use of AI in the fight against sports piracy?

What additional forces in combination with AI influence this fight?

3. State of the Art

This chapter intends to provide information on existing methods of combating piracy of sports streaming content. These include both technological methods like DRM, Watermarking, and AI, as well as legislations that can influence the process

3.1 Digital rights Management

According to Zhang, Cai, and Zhang (2016), for the first time, digital rights were introduced in 1998 and involved various technologies that allowed control and protection of the digital media space. In the early stages, they were the prototype of DRM. As you know, at present, Internet technologies have been widely developed, which has led to the need to control and manage digital content. DRMs serve as the tool that provides service producers with the provision, safekeeping, license phrasing and offer creation, distribution, booking, payment, authorization, and consumption of digital content.

Subramanya (2006), in his work defined the term DRM as a variety of policies, tools and methods that determine the correct use of content. In Figure 4, he showed how the flow of content reaches the consumer from the creator through the producer.

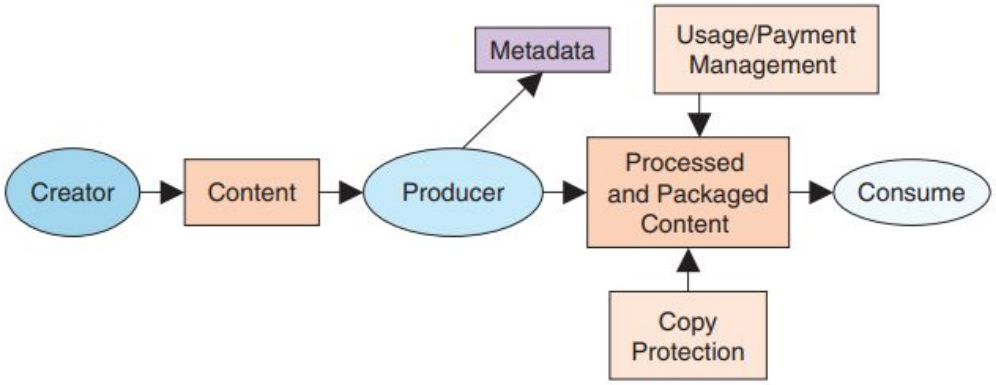

Figure 4. Broad overview of flow of content from creator to consumer

The content producer processes and generates content, which is then delivered to the consumer- the end user. Processed content allows producers to track and manage content usage. DRM plays a key role in this chain, shown in Figure 1, participating in several processes and helping the content creator establish the necessary ownership of content, as well as track content usage and payment information. On the part of the end user, he can choose the desired content and the various options in the use of content. In addition, DRM is a protection technology that can prevent copying and make it impossible for an unauthorized user to consume content (Subramanya, 2016). .

According to Zhaofeng Ma (2017), there are 6 basic requirements for digital rights management. They are called the SACLUP DRM requirement (Table 1) and include:

1. Security;
2. Authentication;
3. Constraint;
4. License;
5. Usage Control;
6. Payment.

№	Requirement	Includes:
1	Security	watermark, encryption of content, hash, digital signature of licence, hash
2	Authentication	usage authentication, identity management by password, certificate of biometric authentication
3	Constraint	permission to use content which depends on the conditions,for instance, whether the user commits valid license request data or pays a specified fee, or satisfies a domain control of use or a period limitation
4	License	release authorization code or XrML file to the user who fulfilled the license constraint and condition
5	Usage Control	DRM user control the content according the license
6	Payment	control the payment process from the user after the content has been transferred to him

Table 1. Basic requirements for DRM

Despite the fact that many academies and research institutes solve the problem of digital resources by representing a single DRM model, in reality, it is difficult to build such a model because there are different content formats. (Zhaofeng Ma, 2017).

Video-oriented DRM model

When it comes to protecting video content, the DRM format is very typical. There are 6 requirements for a typical video-oriented DRM model (see Figure 5):

1. Content encryption;
2. Authentication management;

3. License management;
4. Key management;
5. Protocol supporting;
6. Pay management (Zhaofeng Ma, 2017).

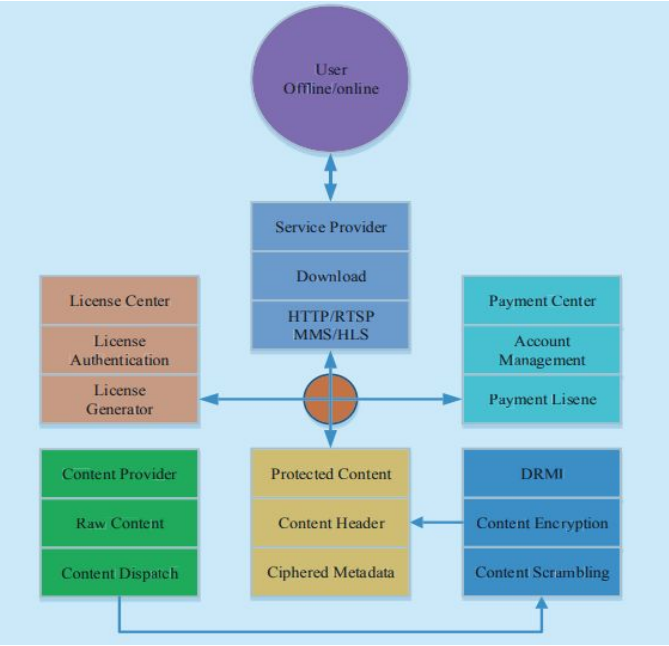

Figure 5. A typical video-oriented DRM model

According to Hofmeister (2019), the most popular DRM systems for protecting video content are:

- "Fairplay: Cipher Block Chaining encryption, only option for Safari and only used by Apple devices.
- Widevine: Developed by Widevine Technologies, bought by Google.
  Used on Android Devices natively, in Chrome, Edge (soon), Roku, Smart TVs, uses protobuf format for metadata.

- PlayReady: developed and maintained by Microsoft. Supported on Windows, most set-top boxes and TVs use WRMHEADER tag objects as metadata format.”

Additional DRM systems are presented in the Figure 6 below (Hofmeister,2019).

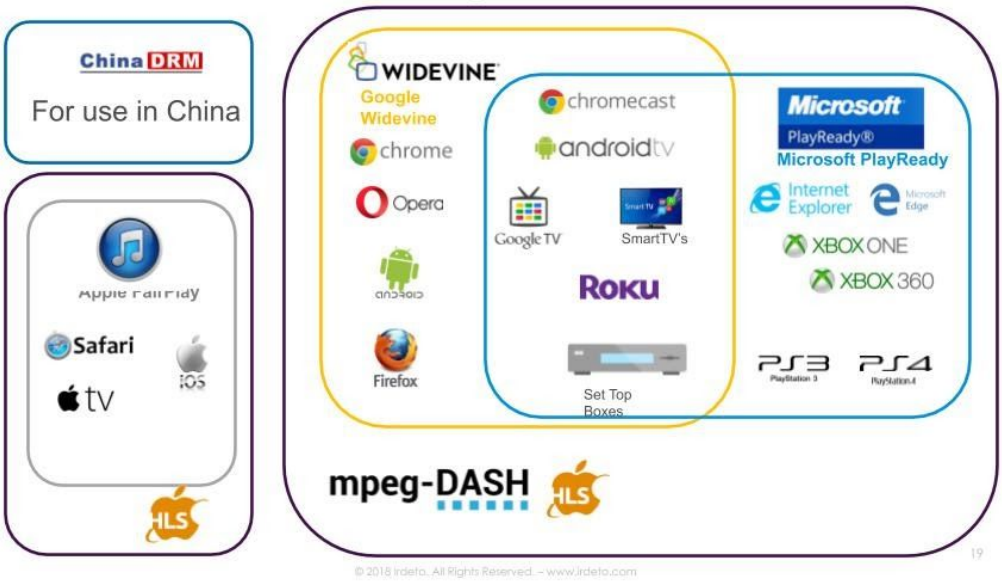

Figure 6. Additional DRM systems

3.2 Image-oriented DRM model (Watermarking)

The digital image is one of the popular formats that are subject to attacks on the Internet and copyright problems is one of serious concerns of the owners of such content. One of the most common protection methods is a digital watermark, which is a technology for embedding marker signals such as images, video, audio into noise-resistant signal objects. The process of using digital watermarks is presented in two steps: embedding the watermark and extracting the watermark (Zhaofeng Ma, 2017).

There are various purposes for using watermarks: copyright protection, **broadcast tracking**, source tracking, information hiding. Depending on the purpose of use, the watermarking techniques are different. There are visible and invisible watermarks. In the first form, the data embedded in the content is visible, such as text or label related to the content owner. Invisible, usually used for audio files. The figure 7 below shows an example of the original image and with the watermark already installed (Kumari, Vijaya & Naidu, 2019).

Figure 7. Example of watermarking

3.3 Artificial Intelligence

Until recently, we could not even imagine such features as image recognition, smart speakers, and self-driving cars. The world has changed so that it can be compared to Wonderland, which was presented in the novels of the British mathematician, recognizable by the name Lewis Carroll. Most of these innovations are possible due to the invention of Artificial intelligence, which penetrates into all aspects of our life and business. AI is “a system’s ability to interpret external data correctly, to learn from such

data, and to use those learnings to achieve specific goals and tasks through flexible adaptation" (Haenlein, Kaplan, 2019).

Poole and Mackworth (2017), explained AI as a field that examines "the synthesis and analysis of computational agents that act intelligently". An agent refers to something that acts in an environment: animals, robots, airplanes, people, organizations, or countries.If it is said that the agent is acting intelligently, it means the following:

- Agent actions are based on the fact that goals, circumstances and consequences are taken into account
- Goals and conditions may change, while the agent remains flexible
- Experience is an important component for an agent and helps to learn.
- Agent makes choices based on calculations and constraints

When it comes to decisions made by agents through computation, such agents are called computational agents. These decisions can be represented as primitive operations implemented on a physical device (hardware). Poole and Mackworth (2017), argue that the goal of AI in engineering is to create and synthesize agents acting intelligently. According to Poole and Mackworth (2017), "Artificial intelligence" refers to the field, but when it comes to the notion of AI there are many misunderstandings since it can be explained as the opposite of real intelligence. The difference is between the origin of intelligence if it occurs in nature, then it is natural, and an artificial one is made by people. At the same time, the mentioned authors argued that it is impossible to have fake intelligence because if there are intelligent agents then they act intelligently. In terms of artificial intelligence, it is real intelligence that was achieved artificially.

3.3.1 Artificial intelligence for fighting piracy

In their work, Stolikj, Jarnikov, and Wajs (2018), stated that illegal broadcasts require constant search and further detection. One of the technologies that enable this to be done is artificial intelligence, which plays a significant role in detecting pirate streams. The

ability of artificial intelligence to apply the semantic analysis of advertising on social networks and web page indexes permits to match the original source with visual elements in the content that is being illegally broadcasted. The visual elements can be logos or images of famous people. The elements differ depending on the type of content such as football matches, films, or new shows, etc.

According to Stolikj, Jarnikov, and Wajs (2018), the process of combating illegal broadcasting consists of 4 steps:

1. discovery of illegal rebroadcasts
2. gathering data from illegal rebroadcasts
3. analyzing data
4. taking measures against rebroadcasters

The first step is to **discover illegal rebroadcasts**. This is done by monitoring and detecting links to illegal broadcasts, which are mainly published on social networks and on indexed websites. These publications contain unified resource identifiers that allow determining the protocol that delivers the web stream or P2P stream (Stolikj, Jarnikov, and Wajs, 2018).

The next step is access to the stream **to collect data** for further verification of the validity of the stream. Depending on the stream protocol, the way to access it differs. The data that is collected is the actual content that is being broadcasted, and stream source identifiers (Stolikj, Jarnikov, and Wajs, 2018).

The previous steps provide an opportunity **to analyze** the collected data to determine the original source. The analysis can be carried out in different ways, such as forensic fingerprinting, watermarking, visual control of the contents, and other methods (Stolikj, Jarnikov, and Wajs, 2018).

The final step, presented by Stolikj, Jarnikov, and Wajs (2018), is **taking action** as an automatic report to an illegal content broadcaster's Internet service provider.

Stolikj, Jarnikov, and Wajs (2018) focused on **analysis of visually identifiable information** (the third step).They presented a system that uses a frame from a

potentially illegal stream as input, then determines whether the frame contains the logo of the original broadcaster for further identification of the logo. The environment of the system is noisy, in which the image quality is distorted, or the logo is not fully visible. As stated by Stolikj, Jarnikov, and Wajs (2018), the latest methods used to detect and recognize logos rely on Convolutional neural networks (CNNs).“ CNNs are a subclass of neural networks which, among other transformations, learn and apply convolutional filters on input data. CNNs are currently state-of-the-art for many image processing tasks, significantly outperforming previous methods based on detecting manually crafted features.” Compared to other methods, the aforementioned method is highly accurate, but at the same time it requires more training data, and the computational requirements are higher (Stolikj, Jarnikov, and Wajs, 2018).

They created a dataset for training and defined methods for detecting and recognizing logos, as existing solutions are not trained to recognize logos in a distorted environment. This process takes place along with constant system adjusting to satisfy requests for new logos and increase recognition accuracy (Stolikj, Jarnikov, and Wajs, 2018).

3.4 Legal methods for sports broadcasts protection

According to Margoni (2016), in accordance with EU copyright law, sporting events are not protected, especially in football matches. Such a decision was made by the EU Court in 2011 in the Premier League vs QC Leisure case. The court also explained that the classification of a sporting event as “author's work” is possible if the corresponding subject is original in the sense of the author’s own intellectual creation.

However, within the meaning of the EU Information Society Directive, **sporting events cannot be considered intellectual creations** (Margoni,2016).

This applies to football matches, which are subject to the rules of the game, thus, these rules do not allow expressing **creative expressive freedom**. The court also stated that sporting events are not protected by European Union law on any other grounds in the

field of intellectual property. Thus, it becomes obvious that the organizers of sports events do not fall under the protection of Art. 81 Copyright Act and are not protected by copyright (Margoni,2016).

In addition, athletes participating in a race or team players are not "performers" in the sense of international, national and EU copyright laws, since the activities they perform are not literary or artistic work (Margoni,2016).

According to Margoni (2016), despite the above-mentioned information, there are remedies that can protect the rights of those who are producers of sports content, as they are involved in the process of creating the broadcast.

A film producer owns economic rights to an audiovisual work in accordance with national law and contractual practices. Sports broadcasts are an audiovisual work, in the process of which many participants are involved. Therefore, the organizers of a sporting event, clubs or federations have the rights to these works, as they are the direct creators of the above content.In the event that there is a third party who has been commissioned for audiovisual coverage, according to the contractual relationship, often the copyright will be transferred back to the club or the creator of the sporting event (Margoni,2016)

Regarding **broadcasting organizations**, they experience protection that provides the ability to prohibit recording, reproduction of recordings and retransmitting using wireless broadcasting facilities, as well as broadcasting television broadcasts to the public. This protection of broadcast signals that contain cinematic or audiovisual work is based on neighbouring rights.

According to Margoni in his article (2016), despite the absence of copyright in the content transmitted by the signal, there are related rights that protect it. Margoni emphasizes that "the signal is protected as such, even if the underlying transmitted material is neither a work of authorship protected by copyright nor other subject matter protected by neighbouring rights." It follows from the foregoing that broadcasts are a protected object, despite the fact that the court may establish that the television game is

not protected by copyright. Margoni also notes that transmitted signals deserve more protection than the content that is transmitted .

Returning to the Premier League vs QC Leisure case, the court ruled that organizations involved in broadcasting sporting events may assert copyright regarding the delivery of a sports broadcast (Margoni, 2016).

According to the European Court, broadcasting organizations can use the right to record their broadcasts to protect their interests, which is provided in art. 7 (2) of the Directive on rental rights, the right to deliver its broadcasts to the public, which is established in Art. 8 (3) of this Directive, or the right to reproduce recordings of its broadcasts, as provided for in Art. 2 (e) InfoSoc Directive (Margoni, 2016).

As for television broadcasting, illegal retransmitting of broadcasts on another channel or the Internet violates neighboring rights. As confirmed by a decision of the European Court in relation to the interpretation of Article 3 (1) The InfoSoc Directive in the event of unauthorized retransmission of television broadcasts over the Internet, the broadcasters' neighboring rights are protected from any public communication activities, including any online broadcasting via **streaming** (Margoni, 2016).

4. Theoretical framework

The purpose of this study is to investigate the potential of using AI in combination with other remedies to combat illegal sports streaming content. After a thorough examination of existing theories, the researcher decided that the most appropriate for this thesis are the Technology Organization Environment (TOE) model and The Pathetic Dot Theory of Lessig.

The reasons for choosing the combination of the theories are based on the ability to consider not only AI contributing to the fight against illegal streaming but also to understand what measures can affect the actions of users, thus the synthesis of all of them will ultimately lead to a decrease in the use of those services.

At this stage, it is necessary to clarify that TOE will be applied to explain the process of adoption of AI in companies involved in the fight and The Pathetic Dot Theory will be used to discover the factors influencing users' attitudes towards illegal services.
The author believed that the chosen theories structure the ideas and intent of this research in comparison with those that are most often used among researchers. To do this, other well-known existing theories that are relevant in similar studies were considered.
The most commonly used theories are the Theory of Reasoned Action (Fishbein & Ajzen, 1975), the Technology Acceptance Model (Davis, Bagozzi, & Warshaw, 1989), the Theory of Planned Behavior (Ajzen, 1985; Taylor & Todd, 1995) and Social-Cognitive Theory (Compeau & Higgins, 1995). The Theory of Reasoned Action explains the behavior of an individual as a consequence of personal intention and social norms affecting him. The Technology Acceptance Model (TAM) argues that the adoption of new technologies depends on consumers, first of all, if they find the technology useful and secondly, easy to use. The Theory of Planned Behavior uses a more sophisticated model and relies on three factors influencing the adoption of innovation, these are attitudes towards acceptance, subjective norm, and perceived behavioral control.
Numerous authors such as Bagozzi (2007), Hu (1999), Wu and Wang (2005), and Pikkarainen (2004) have been criticized the Technology Acceptance Model. This criticism is most clearly presented by Chuttur (2009), who argues that TAM has a “lack of falsifiability, questionable heuristic value, limited explanatory and predictive power, triviality, and lack of any practical” (Chuttur 2009). The reasons why the Theory of Planned Behavior is being criticized are that it is based on cognitive processing and that the needs of potential adopters are ignored until they are interested in a particular action. The emotions of the adopters are also disregarded by this theory as well as by the Social-cognitive theory, which besides assumes that personal change is possible in the presence of changes in the environment, regardless of the motivation of individuals.

Considering the above, the author decided to focus on the (TOE) model and The Pathetic Dot Theory of Lessig, which, in combination with each other, will appear as a Theoretical Framework for this work.

4.1 Technology Organisation Environment model

The research applies the Technology Organisation Environment (TOE) model as part of the Theoretical framework to provide a comprehensive understanding of the potential of adopting Artificial intelligence as a technology for the prevention of the spread of illegal sports broadcasting content in Denmark.

As already mentioned in this paper, Artificial intelligence is a relatively new technological solution for processing a large amount of information and has only just started to conquer various sectors and industries.

The TOE framework was presented by Tornatzky and Fleischer in "The Processes of Technological Innovation" (1990). According to Baker (2011), the wide applicability and explanatory power in various industrial, technological, national/cultural contexts of this model are presented in a number of studies."The TOE model has been used to explain the adoption of inter-organizational systems (Grover 1993; Mishra et al. 2007), e-business (Zhu et al. 2003; Zhu et al. 2006b; Zhu et al. 2004), electronic data interchange (Kuan and Chau 2001), open systems (Chau and Tam 1997), enterprise systems (Ramdani et al. 2009), and a broad spectrum of general IS applications (Thong 1999)". Various industries, such as manufacturing, healthcare, and the financial sector, have used this model to explain the preference of a particular innovation. The major reason explaining the application of the TOE framework in the research is the possibility of analyzing the three elements of technology, organization, and environment that influence the need for new technology application (Baker,2011).

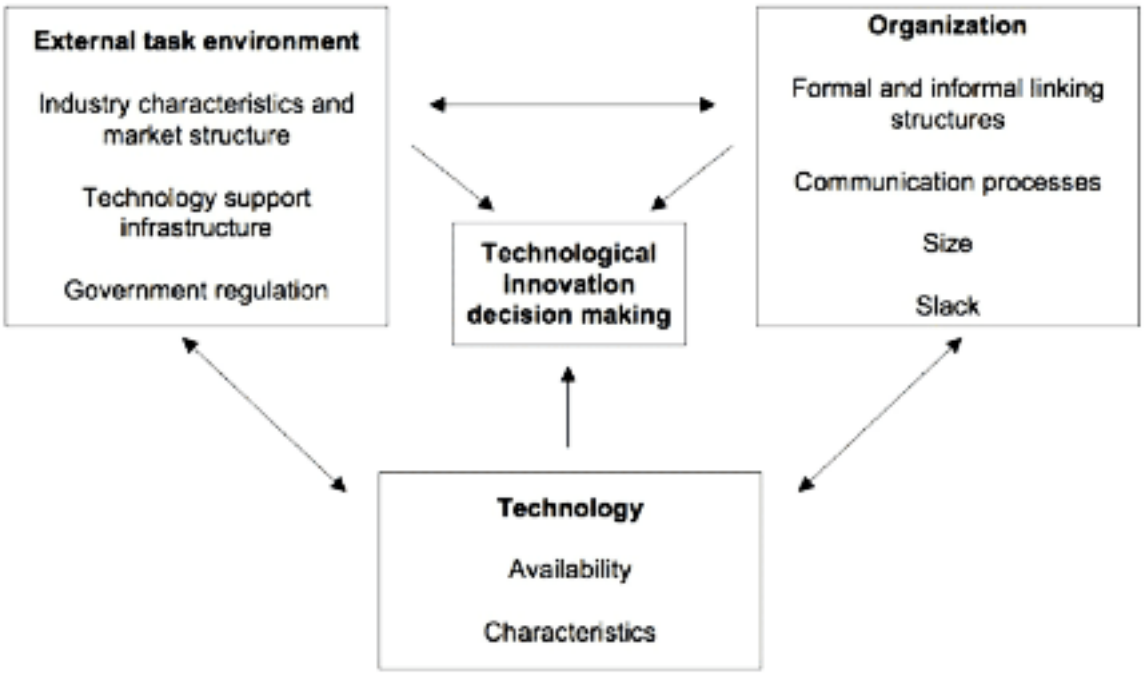

Figure 8. The TOE model

4.1.1 The technological context

The technological context considers available technological innovations in the market, as well as those that are not in use at the time. For the adoption of a certain technology, the key factor is the availability of existing technological tools in a company/industry that can support, strengthen the implementation of innovation (Baker, 2011).

Baker (2011), cited by Tushman and Nadler (1986), divided the changes into three types that will follow after using the new technology:

1. Incremental;
2. Synthetic;
3. Biscontinuous.

Incremental changes are accompanied by insignificant risk and differences in the company that implements the technology, since, in this case, new versions or new features are presented. As examples, Baker (2011), presented the transition to liquid

crystal computer display from cathode ray tube monitors or the implementation of a new version of the enterprise resource planning system in the same company.

Synthetic changes are co-occurred by innovations of medium impact on existing processes. Available solutions are applied in a new form without changing the basic idea of the procedure. For instance, this type of change is the introduction of the use of Internet technology to deliver course content to universities. There is no need for innovation for recording, transmission, and storage in the content of course, but a modern way of technologies combining (Baker, 2011).

Biscontinuous changes bring significant reforms, which entail radical modifications of the processes existing in the company. "Examples include the adoption of bar-code scanning in the grocery industry in the 1970s and 1980s, the change from mainframes to PCs at many corporations in the 1980s, or the shift to cloud computing that began in the early 2000s". These changes can be of two kinds, "competence-enhancing" or "competence-destroying". Competence-enhancing innovations that are introduced in the company allow for consistent changes based on previous experience, which is very different from competence-destroying innovations that result in the complete replacement of existing technology and the obsolescence of numerous types of expertise (Baker, 2011).

4.1.2 The organizational context

The organizational context includes various characteristics of the organization/industry which is considering the possibility of applying new technology. Such characteristics and resources include the structure, methods, and processes of interaction between company employees, the size and availability of free resources. The processes of adoption and implementation are also affected by cross-functional teams and employees who are involved in communication with other offices or participants and partners of the value chain (Baker,2011).

Baker (2011), argues that organizations that have an *organic* and *decentralized* structure are associated with the adoption stage. Organizations with the structures described above are team-oriented and have a softer attitude towards employee responsibility, complementing formal communication between them with sideway communication. The second type of organizational structure that was highlighted is a *mechanical* one, which is characterized by a centralized decision-making process, strictly defined roles of employees, and a fixed method of communication. Organizations following this structuring principle may be most suitable to the implementation stage of a new technology adoption process (Baker,2011).

A crucial role relies on the organization's leadership in establishing the appropriate form of communication. Information on the consequence of making changes to achieve effective company performance or strategy used by top managers can both positively and negatively affect innovation (Baker,2011).

The next factors influencing the support of the idea of the importance of innovation adoption are size and slack. Whereas many studies point that slack promotes the adoption process, other works indicate that the presence of the factor does not necessarily lead to the adoption of technology. The influence of firm size on the adoption of innovation has been widely represented in various studies, despite this, no absolute relationship between this factor and the process of innovative introduction of technology has been found. Large organizations have a greater tendency for innovation compared to smaller ones. One of the central factors is the availability of certain resources that can support decision-making in favor of the use of new technology (Baker,2011).

4.1.3 The environmental context

According to Baker (2011), the environmental context includes factors such as:

1. Industry structure;

2. Availability of service providers;
3. Support infrastructure;
4. Regulatory framework

For example, when it comes to industry structure, competition has a positive effect on the introduction of new technologies, as well as organizations dominating the market can influence the partners of the value chain on the decision to adopt innovation.

It is argued that companies of fast-growing industries tend to positively perceive innovation. As for declining areas, the process of introducing innovations is not so obvious. Thus, part of the organization of declining sectors expects that the effectiveness of the company's processes will increase, while others try to reduce the misuse of finance by avoiding innovative practices. Empirical work confirming these claims about the relationship between the industry's life cycle and innovation has not yet been completed (Baker, 2011).

The support infrastructure of innovation also has an impact. Examples include cases where it is more profitable for companies to replace qualified workers with high salaries by new technologies. Another factor that can support the introduction of innovation is the availability of specialists and consultants who can provide technology implementation services (Baker, 2011).

Government regulations may have both positive and negative effects on the adoption of technology. There are innovations that need to be launched in companies since government restrictions do not permit these companies to continue operating without a particular one. An example is the energy sector, which responsibility is to control the level of pollution that can be carried out by certain technologies. Innovation may be affected by various patents and licenses that increase implementation costs. For instance, in the banking sector, there may be confidentiality restrictions blocking customers from accessing their accounts information. From the above, it follows that the state can play the role of a catalyst or an inhibitor in the processes of technological innovation promotion (Baker, 2011).

In sum, the above three contexts of the TOE framework may provide different impacts on innovative technology, thereby hindering or supporting the development or transition of a company/industry to a new level.

4.2 The Pathetic Dot Theory of Lessig

On the one hand, in this thesis, Artificial intelligence is presented as a fundamental tool to combat the illegal distribution of streaming sports broadcasts. On the other hand, the above-described framework claims that the technology itself does not have the sufficient ability to change a particular process since it is always influenced by certain factors and regulations.

The topic of this dissertation is related to crimes committed by users of cyberspace, who are also influenced by numerous factors that play significant roles in combating piracy. In order to fully reveal the answer to the question of this research, the author decided not to limit the paper by the TOE framework but supports it with The Pathetic Dot Theory that was presented in the book "Codes and Other Laws of Cyberspace" written by Lawrence Lessig in 1999.

Lawrence Lessig participated in many discussions about intellectual property, digital rights and Internet regulations. In his book, he uses the concept of "code is law." According to this principle, the behavior of Internet users is governed by the code by which he means software, as well as the hardware architecture of the Internet. "Code" restricts and structures the actions of people on the Internet. Lawrence introduced a fairly straightforward model that defines the behavior of users or as he called them "pathetic dot". (Lockton,2012).

The model states that 4 modalities of regulation affect any user, precisely "regulable" behavior, not concentrating on cognitive factors. Lessig (1999), argues that by "regulable", he means a certain behavior of a person that can be regulated. This concept is not absolute, since a certain behavior in a certain period of time can be more regulable

than in other circumstances. In his book, he gave an example of gambling, which is less regulated in the Internet space compared to real life.

Returning to the four forces regulating human behavior, these include:

1. Law;
2. Norms;
3. Market;
4. Architecture (Lessig,1999).

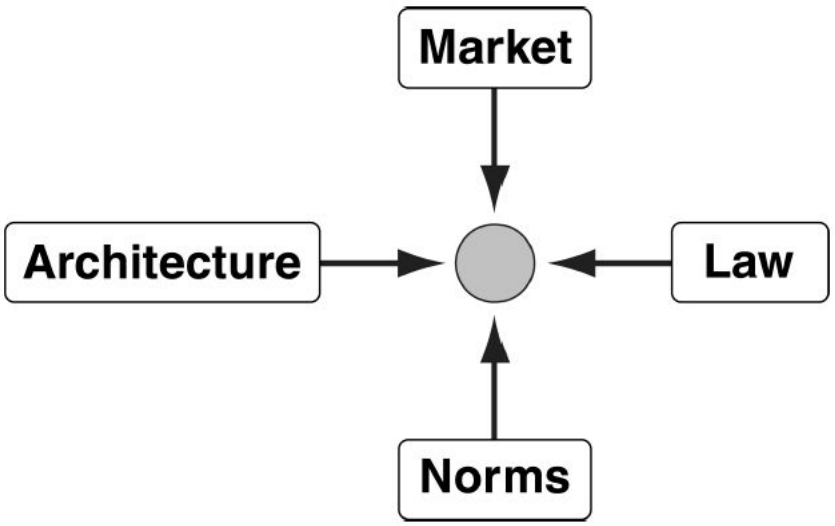

Figure 9. Four forces of Lessig

The law is the remedy that supports legal sanctions that determine a person's behavior leading to avoidance of punishment. Legal punishments include legal sanctions against misconduct and enforcement of legal norms. The resulting effect of these sanctions is certain standards of behavior and penalties in circumstances where a person evades these laws. This allows controlling society while maximizing the freedom of the individual, subject to the mandatory legal framework (Jansen,2019).

Jansen stated that **social norms** are not connected with the law but they can be recognized in real life. According to Lessig (1999), norms restrain the stigma that is imposed by society. "A stigma is an undesirable otherness compared to what we would have expected" (Jansen, 2019).

The next forces represented by Lessig are **market and architecture**. They are not means that impose sanctions but create obstacles. From an economic perspective, the term market is explained as a place, virtual or real, that collects the demand and supply of a particular product and determines prices of goods. Talking about architecture, it is a technical infrastructure that includes physical objects such as building materials, walls."[A]rchitectures constraint through the physical burdens they impose" (Jansen, 2019).

In order to explain the application of this model using a simple example, Lessig (1999), focused on smoking. These four forces influence and regulate the behavior of a smoker. Thus, the law provides for smoking permission (age restriction or special laws that do not allow the purchase of cigarettes), the norms prescribe the behavior of a smoker in certain social circumstances, which may also restrict smoking, such as being in a public place or another person's car. The prices and availability of cigarettes can be regulated by the market. Under Architecture, Lessig presents an example of different types of cigarettes, with a filter, without a filter, strong odors, and smokeless.

According to Jansen (2019), the four modalities described above create a space which detects the most effective legal norms. Thus, it can be noticed how legislative regulations are integrated with various standards, such as social, religious, cultural, economic, and financial, thereby influencing the behavior of individuals in society.

As it was claimed by Jansen (2019), these four modalities are interconnected and depend on each other. Each of these forces can support or limit the other. Technology or architecture may act as a counter to the law or market, but backward support in favor of the law is also possible. The effectiveness of each modality can be of various levels, since the functioning of each may differ. The interaction between modalities is

complicated to represent, due to their complexity. But despite the foregoing, Jansen insists that it is sufficient to understand that they are connected and that they consolidate to regulate the pathetic dot in a certain area.

4.3 The proposed Theoretical framework

For this research, the author has developed a new theoretical framework presented in the figure below, which is a combination of the TOI model and The Pathetic Dot Theory of Lessig. The researcher believes that the model and the theory can complement each other for a structured presentation of empirical data, which will be introduced in the following chapters and ultimately answer the research question.

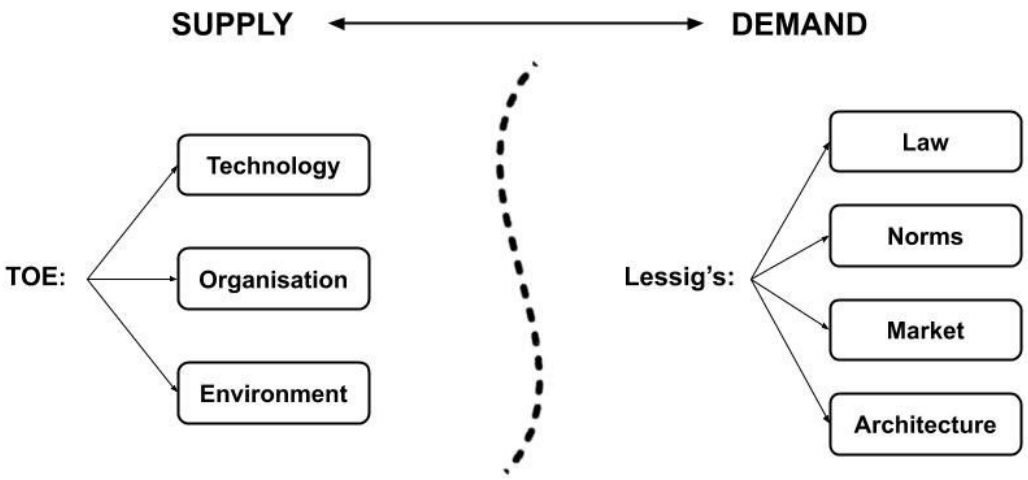

Figure 10. The proposed Theoretical Framework

In the diagram above, the researcher decided to focus on both sides of the streaming service, which includes the owners of the illegal services and the users who watch sports content on those services. They are represented as supply and demand sides, respectively. In the proposed theoretical framework, the TOE model will be used to represent factors related to technological, organizational and environmental contexts that can be applied to combat these streams using Artificial Intelligence. In other words, AI will be seen as the main tool, and the three contexts of the TOE model facilitate the analysis of this solution and the presentation of the factors influencing its application. Despite the fact that in most cases this model has been used to assess the adoption of an innovation in a particular organization, in the case of this study, the main question does not seek to consider the possibility of adoption, but to identify factors that, in combination with components affecting the behavior of the end-user, ultimately will be able to change the existing situation in the area of illegal sport streamings.

As presented by Lessig, the end-user is a pathetic dot that is influenced by external factors and allowed to regulate its actions. As mentioned above, technology by itself does not have a full effect on changing a certain process. The researcher, realizing this, supplemented the TOE model with Lessig's theory, which will help to analyze factors related to the categories of law, norms, market, and architecture. The architecture in this case is an Artificial Intelligence technology that catalyzes the influence of other components on the behavior of the end-user of illegal streaming services.

The researcher believes that after considering the supply and demand sides and identifying factors that, in combination with each other, will be able to answer the questions posed in this study.

5. Methodology

This research is qualitative study and uses methods that are inherent in qualitative research. One explanation for the qualitative study was suggested by Denzin and Lincoln (2005). “Qualitative research is multimethod in focus, involving an interpretative,

naturalistic approach to its subject matter. This means that qualitative researchers study things in their natural settings, attempting to make sense of, or interpret, phenomena in terms of the meanings people bring to them. Qualitative research involves the studied use and collection of a variety of empirical materials – case study, personal experience, introspective, life story, interview, observational, historical, interactional, and visual texts – that describe routine and problematic moments and meanings in individuals' lives (Denzin and Lincoln, 2005). According to Denzin and Lincoln (2003), qualitative research is about interpretation. Qualitative research is multi-method that involves use and collection of different empirical materials and approaches (Aspers and Corte, 2019). In this study, the researcher applied **literature reviews** and **semi-structured interviews** approaches.

Literature review

The literature review is one of the fundamental methods of this research and provides essential information for the reader and the author. This research started with a Literature review, which supported the researcher's original ideas in the **background chapter**. The author, in that chapter, decided to explain to readers where the roots of illegal streaming services come from and the factors affecting their prosperity, as well as explain the principle of operation of pirate websites that provide access to sports broadcasts. Some of the keywords that the author searched for are illegal sports streaming, factors of illegal broadcasts, illegal broadcast, pirated streaming content, fight against illegal streams, illegal sports streams.

The literature review method applied for the **State-of-the-Art chapter** which helped to structure knowledge about the most popular methods of fighting illegal streaming services. As well as searching for information about the background of the research, keywords were used to find academic papers related to recent technologies in the industry. The author used the following pool of keywords: broadcast protection tools,

streaming piracy prevention, technologies for streaming protection, and fighting against illegal digital content. After reviewing the literature on the latest methods and technologies for preventing illegal streaming services, the author singled out DRM, Forensic Watermarking, Fingerprinting, Website Blocking, and AI as the most relevant in the market and presented in the State-of-the-Art chapter.

The next step was to define a **theoretical framework** for this work, which is a crucial part of guiding the research and structuring it in order to present findings in the following chapters.The same approach as for the previous ones was applied to define the theoretical framework.The author reviewed several theoretical and conceptual frameworks, as well as existing academic work in similar fields, which helped the author to create a new theoretical framework that represents a combination of the TOI model and The Pathetic Dot Theory of Lessig. As for the second theory, which complements the theoretical framework, it was chosen after reviewing Lessig Lawrence books: Code and Other Laws of Cyberspace (1999) and Code: Version 2.0 (2006).

Interview processes

To enable the researcher to answer the research questions and have a better understanding of the subject matter, primary data were collected through two semi structured expert interviews.

Interviewees were selected based on their level of expertise in the subject matter.The first interviewee from the Danish Rights Alliance organization. The process of contacting him was not difficult. The researcher found contacts on the website of the organization, and then an interview was conducted with the representative. The process of finding a second interviewee took much longer. First, the author sent emails through the websites of companies that are developing AI solutions to combat streaming services. This approach did not give results, then the author decided to communicate directly with representatives of these companies through the professional social network

Linkedin. In total, about 70 messages were sent out. Ultimately, the Irdeto representative agreed to answer questions and participate in the interview.

Interviewees' details

Interviewee	**Company**	**Role**
Thomas Heldrup	The Danish Rights Alliance	Head of Legal
Werner Strydom	Irdeto	Head of Advanced Technology & Innovation at Irdeto Member of the Supervisory Board at Triggerise

Table 2. Experts' details

Companies' details

The Danish Rights Alliance

The Rights Alliance was founded in 2011 as an interest group fighting to protect the creatives industries' rights and conditions on the Internet in Denmark. It replaced the Anti-Piracy Group, which was closed that year.The Rights Alliance has focused efforts on behavioural and norm changes in users through information and promotions while continuing to enforce against organized criminals and distributors of illegal content (Rights Alliance, 2020)

Irdeto

According to the company's official website, Irdeto is the world leader in digital platform security, protecting platforms and applications for video entertainment, video games, connected transport, connected health and IoT connected industries. Irdeto's solutions and services enable customers to protect their revenue, create new offerings and fight cybercrime effectively. With more than 50 years of expertise in security, Irdeto's software security technology and cyberservices protect more than six billion devices and applications for some of the world's best-known brands (Irdeto, 2020).

Defining the theoretical framework allowed the author to prepare and structure questions for the interviews. Afterwards, the interviews were transcribed and the data was coded using Atlas.ti platform for qualitative data analysis and presented in the next chapters.

6. Collected Data

After finishing the transcribing and coding process of the interviews, the researcher defined 7 main categories:

1. Legislative framework;
2. Techniques of data collection about illegal streamings;
3. Cooperation with third parties;
4. AI application;
5. Challenges in the fight against pirated streaming content;
6. Rights holders challenges;
7. Users' awareness.

№	Category	Summary
1	Legislative	Interviewee 1:

	framework	● The Danish Rights Alliance has recently started taking measures against pirated sport content. Primary focus is on the music and publishing industry; ● The Rights Alliance sues ISPs to deny users access to websites by putting DNS blocks; ● There are also criminal cases against the people behind these cases to stop illegal actions; ● In July 2019, a trial was held in which the Rights Alliance argued that the production of football matches is creative work; ● Danish courts support blocking the websites of illegal streaming that are showing the La Liga, Premier League, Dutch League, all the big football leagues and all kinds of sporting events; ● Article 17 not fully covers illegal services. InfoSoc Directive 2001, Directive 32 is used by Denmarks to protect sports rights holders. Interviewee 2: ● In the past, in Scandinavia there was no legislation to prohibit the use of illegal content, so the lack of relevant legislation led to a large amount of piracy; ● Many countries introduce legislation to support the prohibition of the use of illegal content and support takedown notices, blacklisting and ISPs. From the point of view of existing legislation, this can be a problem. Therefore, it is very important to follow the GDPR and make sure that actions do not violate

		copyright laws and privacy.
2	Techniques of data collection about illegal streamings	Interviewee 1: ● Creating a list of services with links and screenshots of third-party websites with illegal content to present in court to be able to block them; ● Google search engines, Watermarking, DRM,Facebook Rights Management. Interviewee 2: ● Technologies for creating large pools of IP addresses to avoid blocking from pirates. Every IP address is used for a short period of time and then is discarded; ● Selenium is an open-source technology for building web crawlers. Web crawlers are technologies that use keywords to detect illegal websites; ● Web crawling allows to switch quickly from one website to another; ● The company tracks illegal streaming and downloading. Before the process of tracking was human-intensive. After the first step of applying web crawlers to collect the links of illegal websites, analysts start processing each link, whether they are sport, movie, TV series. They have to see if it is content that the company is responsible for protecting; ● After shutting down illegal websites, it takes time

		to create new ones and it slows down piracy.
3	Cooperation with third parties	Interviewee 1: ● Cooperation with La Liga and ISPs. ● La liga is a partner that has about 20 specialists in the antiparacy technical team who are monitoring all different kinds of sites and seeing where La liga matches are; ● ISPs should block not only services which is currently on a website, but also future services that provide the same content; Interviewee 2: ● Cooperation with ISPs to take down the content. ● If a takedown notices or issue was a mistake, then the company may lose trust from Internet providers. Therefore, it is necessary to build trusting relationships with ISPs.
4	AI application	Interviewee 1: ● AI can work with image recognition. Interviewee 2: ● Analysts work partially replaced by AI. AI narrows down the detection process by adding metadata everytime when it detects the language, type of sport or logo. Neural networks are used for image recognition. ● Relatively not expensive solution in comparison with the amount of earnings that the broadcasters

		lose because of pirates and the price is reasonable in order to keep customers; ● AI takes a lot of data to train a model. For Irdeto is not a problem, because the company has been training the model for years; ● It takes 5-10 minutes to detect illegal live sports streaming and to send a take down notice; ● AI is not a threat that comes to destroy jobs. It's empowering analysts and helping them to look at a larger number of websites. It's human augmentation, not human replacement; ● There are 10-20 well-known companies in the world providing the same protection in the industry.
5	Challenges in the fight against pirated streaming content	Interviewee 1: ● It is impossible to prevent everything from being put on the Internet illegally; ● The illegal website is easy to duplicate by changing the domain name; ● It is a long battle. Interviewee 2: ● ISPs are not really interested in blocking illegal websites because they don't really care if users are running a website that's showing pirated content or they're running a webshop; ● Finding an illegal website is not a problem for users, because there are a lot of commercials on the

		Internet advertising the products; ● It is a cat and mouse game.
6	Rights holders challenges	Interviewee 1: ● Threats for the ability to make new sport content. Interviewee 2: ● There are sports rights holders like Formula One, the Premier League which sell content to broadcasters. Broadcasters are the end customers of piracy prevention companies; ● The sports teams will stop being able to afford good players because of the presence of illegal services which make the content free to watch.
7	Users awareness	Interviewee 1: ● There will always be users who will not pay for content, but there is a large audience who may not be aware that it is illegal and can be encouraged to use legal content; ● Not all users are informed about the malware on the illegal streaming services. 50-60 % of ads are infected with malware; ● Users are not aware that the services are not free, they are paying with their personal identity; ● Share with Care campaign is shown on already blocked websites to explain users the rights and consequences of not using legal sources. Interviewee 2: ● Legal content should be easily accessible and at

		reasonable price making the access to pirated content difficult; ● There can be problems if the sports content for different countries are not accessible.

Table3. Summary of interviews

7. Analysis and discussions

This chapter intends to provide an analysis and discussion of the data collected during the interviews with experts from The Danish Rights Alliance and Irdeto, an anti-piracy company. For this, the researcher applied the previously presented Theoretical Framework (Figure 10), which will help to consider the two sides of the process associated with watching illegal sports matches and events. One side represents users, respectively, pirates and the second is the combination of techniques (special focus on AI) of fighting them and illegal services. The analysis begins with the application of The TOE model. The purpose of which is to present the researcher's findings on the application of AI, then the author turns to the Lessig theory, with the help of which the author will analyze the side of the users of illegal services.

7.1 The TOE model

According to the TOE model presented in the paper, there are 3 contexts influencing the adoption of a specific technology. As it was mentioned before, the research is not intended to analyze the adoption process, however, the TOE model helps to understand the factors impacting the use of AI within the industry. Particularly, as it was described by interviewee 2, Werner Strydom from the Irdeto company, customers of AI solutions combating piracy of sports streamings are commonly operators that broadcast sports content.

The technological context

To examine the impact of the technological context on the use of Artificial Intelligence, the author decided to give an example of the process of combating illegal streaming in The Danish Rights Alliance, which currently do not use this technology in their organization to fight pirated websites, but cooperate with La Liga, which provides them with a list of already found illegal services for further actions to prevent the spread of such content. The chain of measures used in this organization is shown in the figure below. It should be mentioned, the author has no information on what method La Liga specialists use to detect illegal streaming.

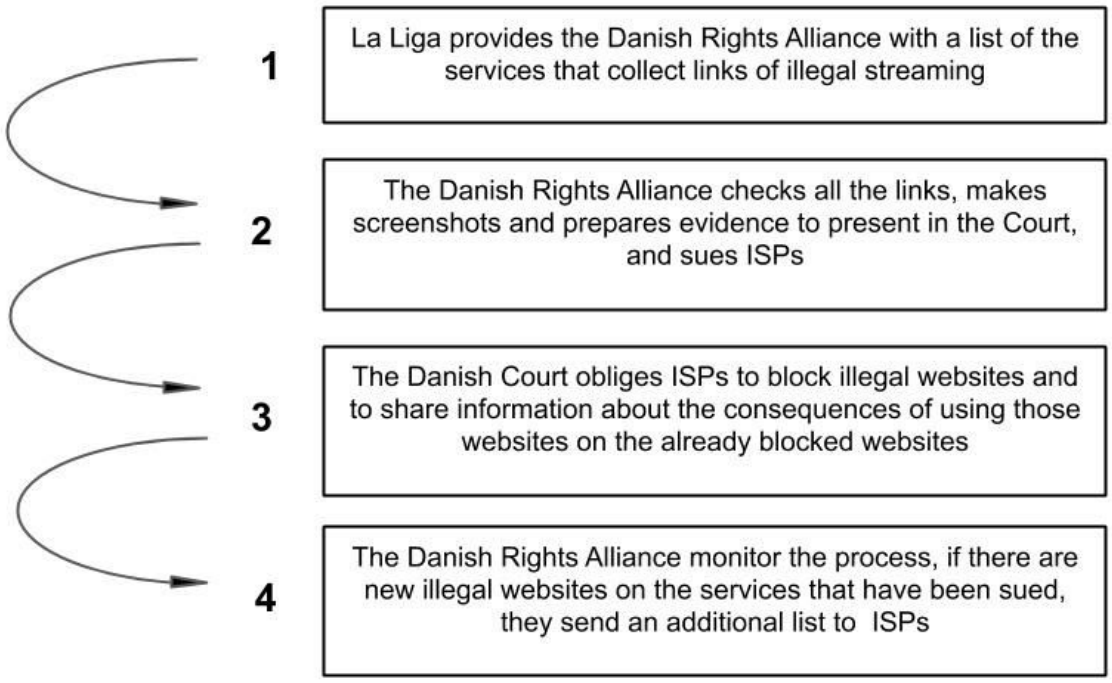

Figure 11. Chain of actions in the Danish Rights Alliance

As stated during the interview with Thomas Heldrup, sports content is not the main focus of this organization: " It's the music industry, the publishing industry. At the moment, we don't have sports rights as primary members but we're working on that." However, Thomas also said that they have recently started working with La Liga: "It was last year and we started this collaboration with La Liga and the blocking because of a positive blocking case."

At the moment, starting from the second step, all the further processes involve representatives of the alliance using their own infrastructure. After getting the list from La Liga, experts check each link to prepare evidence such as screenshots and domain names to be taken to court, where they sue ISPs to block these websites.

The information provided on the sequence of actions in the alliance shows that at the moment this organization does not use AI in any steps. But the author implies that the

use of this technology could lead to changes in the alliance, or in another organization involved in the prevention of illegal sports streaming. For comparison, below is Figure 12, which represents the anti-streaming piracy chain of action at Irdeto, which provides services to interested companies and organizations.

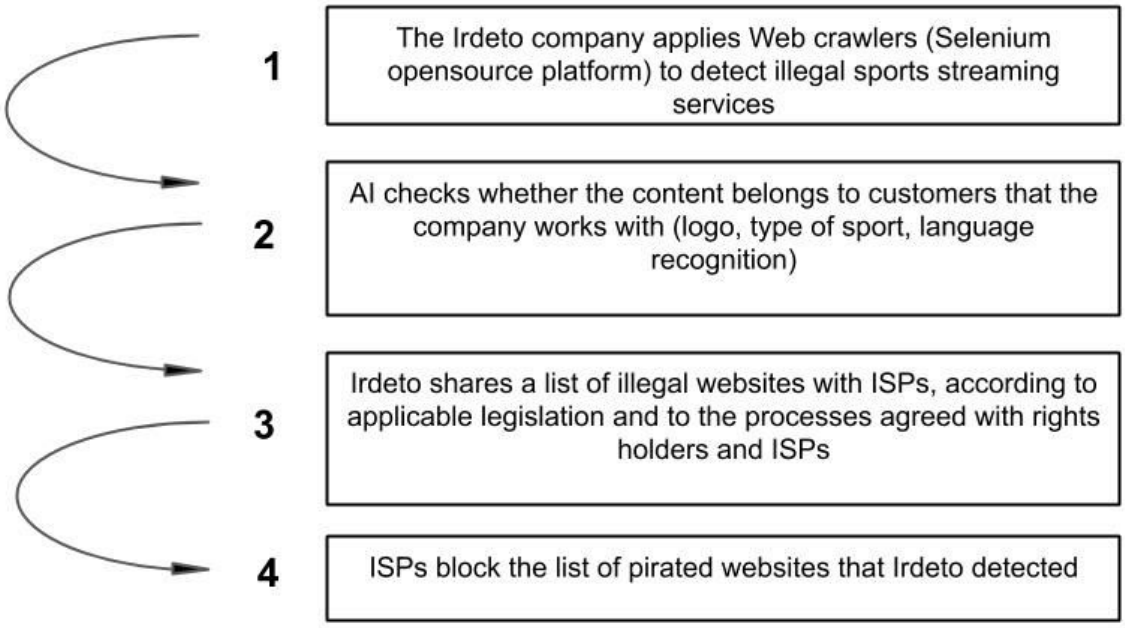

Figure 12. Chain of actions in the Irdeto

According to the interview with Werner Strydom from Irdeto, the first step begins with the use of technologies that search for illegal resources distributing sports streaming content. The first technology is web crawlers. In particular, Irdeto uses the Selenium platform. Werner described it as " a library with functions that you can quickly put together a small program that can look at the content of a website, go through all of the information, all of the links on a website, and by using keywords, filter out certain bits of information that you need. Selenium is like a library that you can use to build these little web crawlers. Selenium is open-source, but the web crawler that we built is our solution."

In the second step, Artificial Intelligence gets down to business, which takes on the task of analyzing the information found. As the second interviewee said, this process was previously human-intensive and involved the active implications of analysts: “Then analysts have to look at each link that they find to see what content is this. Is it a movie? Is it a TV series? Is it sports? Then they have to see if it is content that we are responsible for protecting. So they have to look to see who is the broadcaster, because it could be, for example, that a sports event is a popular sports event and it's available on ten different broadcasters at the same time. But we are only being paid by one of those broadcasters.”

Currently, Irdeto is automating the above process using AI. As it was also described in the chapter State-of-the-Art, Stolikj, Jarnikov, and Wajs (2018) explained the use of AI to analyze content that was detected. In their case, they use the Convolutional Neural Network to define the logo for a specific sports broadcast.

At Irdeto, AI is also used to analyze the type of sport. Werner said: “We built a machine learning model that can recognize certain types of sports. So a sports classifier basically is what we did. It's only trained to recognize a small number of sports, but it can distinguish, for example, football from hockey and from tennis. ” In addition, their technology has the ability to detect the translation language.

As it was stated by Stolikj, Jarnikov, and Wajs (2018), AI requires more training data, and the computational requirements are higher. In this regard, Werner mentioned: “There is more data than we can ever use. And we've been doing this for many years. And so the amount of data that's available to train AI is huge.”

With regard to the definition of the technological context of the use of AI, the author can conclude that this technology requires changes in the company, especially if the company does not have experience in using AI in the fight against streaming services. As described in the theoretical framework, there are three types of changes that follow after the introduction of an innovation or technology in an organization. They can be incremental, synthetic, discontinuous.

After presenting the technological features of the use of AI at Irdeto, the researcher suggests that the changes will be synthetic. Because synthetic changes have a medium impact on existing processes and do not affect the basic ideas of a certain procedure, which will undergo the introduction of new technology. Bearing in mind that The Rights Alliance has a similar chain of actions as in Irdeto and these organizations have the same goal in the industry, this is the fight against piracy in the Internet space, the author can presume that the changes will affect the process of analyzing the collected information about illegal streaming. In other processes, a company defines its own priorities and steps.

The organizational context

Bearing in mind that this study does not intend to study the implementation of AI in a particular organization, it uses the TOE model to determine the potential factors influencing the use of AI, it should be noted that this part will rely on the opinions of experts obtained during the interviews.

According to Baker (2011), the organizational context combines different characteristics such as the structure, methods, and processes of interaction between company employees, the size and availability of free resources.

As it was already revealed above, the use of AI leads to synthetic changes, that is, to medium ones, and does not change the basic procedures, particularly in the regard of the research, for analyzing collected illegal web services, and also does not affect internal processes related to interaction within the organization, but only automates one of the processes pointwise in the chain of the fight against pirated streaming services.

In terms of organizational structure, this characteristic has the least impact on the use of AI in the context of this study. According to Werner, in the process of using AI, only one process is automated that was previously processed by analysts, the process of determining the relevance of illegal streaming, that is, whether streaming is the content that customers are interested in.

As was stated by Baker (2011), the organization's leadership process plays an essential role in making a decision about the adoption of a certain technology. Effectiveness of company performance and strategy applied by a leadership team can affect the implementation of new technology.

During the second interview, Werner said that every company interested in using AI against illegal sports broadcasts should determine the benefits for the company itself: "What they need to do is they need to weigh it against the benefit they get from it. And that's always a very difficult calculation to do. So if you have a sports event and you don't do anything to protect the illegal broadcast, what is the impact on the sport, on the broadcaster? Will they get one percent more viewers? Will they get 10 percent more viewers? " He also noted that the calculations are mostly done by the companies themselves, but it is interesting to highlight the following: "So what we can see is that for high profile events like big games, La Liga, Premier League, the Formula One races, certainly, that's worth it. But for local soccer teams, for less popular sporting events, it's not worth the trouble. " According to Baker (2011), large organizations have a greater tendency for innovation compared to smaller ones. From the above, it can be assumed that, to a greater extent, large organizations that broadcast matches, as well as sports organizations selling the right to broadcast these events, will be interested in artificial intelligence as a solution against illegal sports broadcasts.

The environmental context

To address this context, the author recalls the factors related to it:

1. Industry structure;
2. Availability of service providers;
3. Support infrastructure;
4. Regulatory framework

When it comes to the **structure**, the sports industry is one of the largest, which annually loses a huge amount of money from watching illegal broadcasts. As introduced in the

Background chapter, in 2017 alone, Danish IP addresses visited pirated sites with live streaming of sports matches 2.96 million times, which is almost 250,000 monthly visits. The Danish Rights Alliance is the only anti-piracy group representing local and international rights holders in Denmark and preventing the spread of illegal streamings. It can be assumed that the structure of the industry does not play a key role in deciding whether to ap[ply the technology discussed in this thesis. According to Baker (2011), competition has a positive effect on the introduction of new technologies, as well as organizations dominating the market can influence the partners of the value chain on the decision to adopt innovation. As for Denmark, both are lacking in this industry.

In terms of **availability**, Werner mentioned that there are 10-20 well-known companies in the world doing anti-piracy activities and providing protection and that Irdeto can not charge a lot of money: “Every single broadcaster can easily afford the solution that it's not a very high cost. We're not talking about thousands of dollars, not hundreds of thousands of dollars. We can't charge a lot of money for this service. It's not an expensive service because if we charge too much, they can still go to another company.” As for the implementation and use of this technology by representatives of the interested company, as Werner said, the company itself must determine how it will be profitable for it, buy a ready-made service or hire/retrain employees to support the service.

The **support infrastructure** in the case of this study is one of the essential parts. As it was stated above, in the chain of activities for prevention pirated content involved third parties and additional technologies. Before moving on to the use of AI to analyze found pirate streams, it is required to use technologies to find services that provide links to these streams. In the case of the Danish Rights Alliance, this list is provided to them by La Liga. In the Irdeto that provides a ready-made service, these are done by web crawlers technology. According to Werner, “the gathering data is done with crawlers. That's an automated process. Crawlers are given some keywords and it'll go and try and find the links to files and streams that are illegal.” The solution is located in the cloud space, which should also provide the infrastructures for operating the solution. At Irdeto,

the solution runs at Amazon Web Services. They also have to use technologies for creating large pools of IP addresses to avoid blocking from pirates. Every IP address is used for a short period of time and then is discarded. Also, the logo must be installed on the broadcast, this should be done by the operators-broadcasting organizations applying watermarking. Thomas Heldrup in the interview mentioned DRM, Facebook rights management, and Google search engines as additional technologies to take up the fight. Cooperation with ISPs is the final step in the fight against Internet piracy. As Werner said, not all ISPs are interested in blocking these websites because they don't really care if they're running a website that's showing illegal content or they're running a webshop. In the Danish case, ISPs are obliged by the court to block illegal streaming and also post a notice on already blocked sites about the consequences of using these resources, which implies the cooperation of The Danish Rights Alliance with ISPs to obtain the desired result.

According to Baker (2011), the **regulatory framework** of the environmental context implies that the state can have both positive and negative effects on the use of a particular technology. In the interview with a second expert, it was said that many states are implementing legislation that supports the fight against Internet piracy by allowing blocking, sending takedown notices, and blacklisting. It was also mentioned by him that in the past, in Scandinavia there was no legislation to prohibit the use of illegal content, so the lack of relevant legislation led to a large amount of piracy. Nowadays, The Danish Rights Alliance struggles with these consequences and they claim that they manage to resist the pirates.

At the same time, they defend the rights of sporting events to be called creative work, in order to enforce the Art. 81 Copyright Act. As previously presented in the chapter State-of-the-art, in the European space, sports broadcasts are not protected by law and have no right to be protected by a court. According to Margoni (2016), within the meaning of the EU Information Society Directive, sporting events cannot be considered intellectual creations. In July 2019, a trial was held in which the Rights Alliance argued

that the production of football matches is creative work. Thomas said: “Traditionally or at least in the legal discourse, it has been questioned whether or not sporting events could be protected by copyright because players and the whole game are dictated by rules. And it means you can argue that there's no room for anything creative in that. But what we are arguing is that in the production of the football matches, there is a creative aspect because there are so many cameras on the stadium and the production team can also apply logos and graphics, and sound. ”

When it comes to the existing legislation, Werner said that it can be a problem. Therefore, it is very important to follow the GDPR and make sure that actions do not violate copyright laws and privacy.

The legislative framework also plays an important role in applying The Pathetic Dot Theory of Lessig which is presented below.

7.2 The Pathetic Dot Theory of Lessig

According to Lessig (1999), there are four forces influencing human behavior. In the study, users of illegal sports streaming services are presented as pathetic dots which are influenced by forces such as:

1. Law;
2. Norms;
3. Market;
4. Architecture.

In addition to what is already presented above regarding laws and regulations, users of pirated content are also prosecuted in Denmark. In the interview with a spokesman for The Daish Rights Alliance, it was said: “There are also criminal cases brought against the people behind these cases as well to try and really stop them”.

Regarding the norms, it was stated by Jansen (2019), that they are not connected with legal regulations but can be recognized in real life. Thomas Heldrup claimed: “It is

impossible to prevent everything from being put on the Internet illegally". According to him, there always will be users who don't want to pay the price of content, but the big part of the audience who maybe don't know that it's illegal or who just got a link from a friend can be nudged to use legal content instead. Werner Strydom said on this occasion: "I think I have no sympathy if you're able to afford the content and you're not paying for it, then you're actually destroying the future of that sport with that content. If all of the Disney content was pirated and nobody paid for it, then Disney will stop making content and the sports teams will stop being able to afford good players."

The Danish Rights Alliance is working with the Ministry of Culture to raise awareness of the consequences of using illegal resources through the Share with Care campaign, which is displayed when users try again to open an illegal website that has already been blocked. It explains that in fact, these illegal resources are not free, users pay with their confidential information, in addition, they infect their computers with malware, which is stored in 50-60% of the ads displayed on these websites.

Market and architecture are also an important part of this theory. According to the second expert interviewed, access to legal content should be easy. As he gave the example of users forced to watch illegal broadcasts from their home states because they are unable to find legal access in the country they are located in. He also noted the prices for legal services should be reasonable and affordable.

In terms of architecture, The Danish Rights Alliance is trying to make accessing illegal content as difficult as possible. From this perspective, Irdeto's AI solution has a positive impact on fighting. As Werner said, on average, it takes 5-10 minutes to prevent illegal streaming from the moment it starts. Meanwhile, the user has to re-search for pirated resources to watch illegal sports broadcasts, which slows down piracy.

8. Answering the research questions

To gain a better understanding , it is important to mirror the research questions:

Main Question:

What is the role of AI in the battle against illegal sports streaming services ?

Sub Questions:

What factors are driving the use of AI in the fight against sports piracy?

What additional forces in combination with AI influence this fight?

According to the theoretical framework proposed by the author of the study, which is a combination of The TOE model and The Pathetic Dot Theory of Lessig separating the process of using of illegal streaming sports resources on the supply and demand parts (in particular, the supply side is services that provide access to the mentioned content and the demand side are users of these services), it can be concluded that the questions posed in this thesis are disclosed and answered.

Regarding the main question about the role of AI in the fight against pirate sports streamings, the author analyzed the chain of actions used by The Danish Rights Alliance and Irdeto, which offers a solution using AI. As a result, AI is currently being used in the step of analyzing collected links to illegal websites, which automates a process that was done manually by analysts in the past. As it was said by the representative of Irdeto Werner Strydom, they are now able to identify these sites in approximately 5-10 minutes from the start of the sports broadcast, with the help of Internet providers who are responsible for the last step - blocking these sites.

It should also be noted that the turn of AI, in this case, comes after the use of technologies for collecting links; additional tools are also required for a full-fledged fight. An important role is given to well-coordinated work with ISPs, which, in the case of Denmark, are obliged to block and notify users about the consequences of using illegal resources.

In answering the sub questions, The TOE model helped to identify factors related to technological, organizational and environmental contexts.

The anti-piracy solution for the sports broadcasting industry is present in the market and available to interested organizations. Every company potentially considering implementing this solution can weigh the pros and cons. In most cases, customers are sports content broadcasters or right holders of this content who have the resources to afford this technology. Regarding legal tools, in Denmark, there are real cases supported by legislation that can positively influence the decision-making process on the use of AI. The Pathetic Dot Theory of Lessig complemented The TOE model and helped examine the factors influencing end-user behavior in the context of law, social norms, market and architecture. Danish law already supports blocking illegal resources, and The Danish Rights Alliance is conducting user awareness campaigns and disseminating information about the possible consequences of using illegal resources, such as malware, the threat of theft of confidential information, and prosecution.

9. Conclusion

Currently, piracy in the Internet space is a big threat. In particular, with regard to this study, the author examined the situation of the use of illegal streaming services for watching sports matches in Denmark. As presented in the thesis, these services can negatively affect the sports industry as a whole, because every year fans of sports events choose to use pirated resources, thereby reducing the views of legal broadcasts, which does not bring profit to the sports industry and affects its viability. In this work, the author presented data on the situation in Denmark, and also considered methods of fighting pirates. A special focus was on the use of AI as a tool that, in combination with other forces such as law, market, social norms, is able to resist watching illegal content.

10. Bibliography

Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior. Action Control, 11–39. https://doi.org/10.1007/978-3-642-69746-3_2

Aspers, P., & Corte, U. (2019). What is Qualitative in Qualitative Research. Qualitative Sociology, 42(2), 139–160. https://doi.org/10.1007/s11133-019-9413-7

Bagozzi, R. (2007). The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift. Journal of the Association for Information Systems, 8(4), 244–254. https://doi.org/10.17705/1jais.00122

Baker, J. (2011). The Technology–Organization–Environment Framework. Information Systems Theory, 231–245. https://doi.org/10.1007/978-1-4419-6108-2_12

Chau, P. Y. K., & Tam, K. Y. (1997). Factors Affecting the Adoption of Open Systems: An Exploratory Study. MIS Quarterly, 21(1), 1. https://doi.org/10.2307/249740

Chen, J. (2020, March). Lemons Problem. Investopedia. https://www.investopedia.com/terms/l/lemons-problem.asp

Chuttur, M. (2009). Overview of the Technology Acceptance Model: Origins, Developments an" by Mohammad Chuttur. AIS ELibrary. https://aisel.aisnet.org/sprouts_all/290/

Compeau, D. R., & Higgins, C. A. (1995). Computer Self-Efficacy: Development of a Measure and Initial Test. MIS Quarterly, 19(2), 189. https://doi.org/10.2307/249688

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. Management Science, 35(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

Fishbein, M., & Ajzen, I. (1975). Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research (Addison-Wesley series in social psychology). Addison-Wesley.

Grover, V. (1993). An Empirically Derived Model for the Adoption of Customer-based Interorganizational Systems. Decision Sciences, 24(3), 603–640. https://doi.org/10.1111/j.1540-5915.1993.tb01295.x

Haenlein, M., & Kaplan, A. (2019). A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. California Management Review, 61(4), 5–14. https://doi.org/10.1177/0008125619864925

Hofmeister, W. (2020a, May 12). Digital Rights Management (DRM) - Everything you need to know. Bitmovin. https://bitmovin.com/digital-rights-management-everything-to-know/

Hofmeister, W. (2020b, May 12). Digital Rights Management (DRM) - Everything you need to know. Bitmovin. https://bitmovin.com/digital-rights-management-everything-to-know/

Hoof, L. (2016). Live sports, Piracy and Uncertainty: Understanding illegal streaming aggregation platforms (null ed.). Institute of Network Cultures.

Hsiao, L. (2019, January 3). The Price of Free Illegal Live Streaming Services. ArXiv.Org. https://arxiv.org/abs/1901.00579

Hu, P. J., Chau, P. Y. K., Sheng, O. R. L., & Tam, K. Y. (1999). Examining the Technology Acceptance Model Using Physician Acceptance of Telemedicine Technology. Journal of Management Information Systems, 16(2), 91–112. https://doi.org/10.1080/07421222.1999.11518247

Irdeto. (2020, October 30). Irdeto. https://irdeto.com/about-us/#whoweare

Jansen, B. (2019). Towards a Hermeneutics of Pathetic Dots : Finding the Gap Between Law and Reality. Yuridika, 34(3), 419. https://doi.org/10.20473/ydk.v34i3.14948

Kariyawasam, K., & Tsai, M. (2017). Copyright and live streaming of sports broadcasting. International Review of Law, Computers & Technology, 31(3), 265–288. https://doi.org/10.1080/13600869.2017.1299553

Kokorina, T. (2017). All about the fight against piracy. How not to lose millions on illegal broadcasts. Sport-Connect.Ru. http://sport-connect.ru/case/piratstvo

Kuan, K. K. Y., & Chau, P. Y. K. (2001). A perception-based model for EDI adoption in small businesses using a technology–organization–environment framework. Information & Management, 38(8), 507–521. https://doi.org/10.1016/s0378-7206(01)00073-8

Kumari, R. R., Vijaya, V., & Naidu, K. R. (2019). Existing Trends of Digital Watermarking and its Significant Impact on Multimedia Streaming: A Survey. International Journal of Advanced Computer Science and Applications, 10(2), 126–139. https://doi.org/10.14569/ijacsa.2019.0100217

Leporini, D. (2017). Architectures and protocols powering illegal content streaming over the internet. IBC. https://www.ibc.org/architectures-and-protocols-powering-illegal-content-streaming-over-the-internet/1026.article

Lessig, L. (1999). Code: And Other Laws Of Cyberspace by Lawrence Lessig (1999-11-30). Basic Books.

Lobato, R., & Meese, J. (2016). Geoblocking and Global Video Culture (null ed.). Institute of Network Cultures.

Lockton, D. (2012). Persuasive Technology and Digital Design for Behaviour Change. SSRN Electronic Journal, 1. https://doi.org/10.2139/ssrn.2125957

Margoni, T. (2016). The Protection of Sports Events in the EU: Property, Intellectual Property, Unfair Competition and Special Forms of Protection. IIC - International Review of Intellectual Property and Competition Law, 47(4), 386–417. https://doi.org/10.1007/s40319-016-0475-8

Mishra, A. N., Konana, P., & Barua, A. (2007). Antecedents and Consequences of Internet Use in Procurement: An Empirical Investigation of U.S. Manufacturing Firms. Information Systems Research, 18(1), 103–120. https://doi.org/10.1287/isre.1070.0115

Nybom, K., & Skov-Jensen, M. (2018, August 31). Tikkende bombe under dansk fodbold: Stadig flere ser kampe på nettet uden at betale. DR.

https://www.dr.dk/nyheder/regionale/midtvest/tikkende-bombe-under-dansk-fodbold-stadig-flere-ser-kampe-paa-nettet-uden

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., & Pahnila, S. (2004). Consumer acceptance of online banking: an extension of the technology acceptance model. Internet Research, 14(3), 224–235. https://doi.org/10.1108/10662240410542652

Poole, D. L., & Mackworth, A. K. (2017). Artificial Intelligence: Foundations of Computational Agents, 2nd Edition. Cambridge University Press. https://artint.info/2e/html/ArtInt2e.html

Ramdani, B., Kawalek, P., & Lorenzo, O. (2009). Predicting SMEs' adoption of enterprise systems. Journal of Enterprise Information Management, 22(1/2), 10–24. https://doi.org/10.1108/17410390910922796

Stolikj, M., Jarnikov, D., & Wajs, A. (2018). Artificial Intelligence for Detecting Media Piracy. SMPTE Motion Imaging Journal, 127(6), 22–27. https://doi.org/10.5594/jmi.2018.2827181

Subramanya, S. R., & Yi, B. K. (2006). Digital rights management. IEEE Potentials, 25(2), 31–34. https://doi.org/10.1109/mp.2006.1649008

Taylor, S., & Todd, P. A. (1995). Understanding Information Technology Usage: A Test of Competing Models. Information Systems Research, 6(2), 144–176. https://doi.org/10.1287/isre.6.2.144

The Danish Rights Alliance. (2018, April). The Danish Rights Alliance annual report 2017. https://rettighedsalliancen.dk/wp-content/uploads/2020/04/RettighedsAlliancens-a,PCC,P8Arsberetning-2017-English.pdf.pagespeed.ce.i7bprV26aN.pdf

The Danish Rights Alliance. (2019, April). The Danish Rights Alliance annual report 2018. https://rettighedsalliancen.dk/wp-content/uploads/2020/04/rettighedsalliancens-annual-report-2018-.pdf.pagespeed.ce.Kk21FUPiPf.pdf

The Rights Alliance. (2020, June 30). Our story. RettighedsAlliancen. https://rettighedsalliancen.com/our-story/

Thong, J. Y. L. (1999). An Integrated Model of Information Systems Adoption in Small Businesses. Journal of Management Information Systems, 15(4), 187–214. https://doi.org/10.1080/07421222.1999.11518227

Tornatzky, L. G., & Fleischer, M. (1990). Processes of Technological Innovation (Issues in Organization and Management Series). Lexington Books.

Tushman, M., & Nadler, D. (1986). Organizing for Innovation. California Management Review, 28(3), 74–92. https://doi.org/10.2307/41165203

Wu, J.-H., & Wang, S.-C. (2005). What drives mobile commerce? Information & Management, 42(5), 719–729. https://doi.org/10.1016/j.im.2004.07.001

Zhang, J., Cai, J., & Zhang, Z. (2016). A Novel Digital Rights Management Mechanism on Peer-to-Peer Streaming System. Advances in Intelligent Information Hiding and Multimedia Signal Processing, 243–250. https://doi.org/10.1007/978-3-319-50209-0_30

Zhaofeng Ma. (2017). Digital rights management: Model, technology and application. China Communications, 14(6), 156–167. https://doi.org/10.1109/cc.2017.7961371

ZHU, K. E. V. I. N., KRAEMER, K. E. N. N. E. T. H. L., & DEDRICK, J. A. S. O. N. (2004). Information Technology Payoff in E-Business Environments: An International Perspective on Value Creation of E-Business in the Financial Services Industry. Journal of Management Information Systems, 21(1), 17–54. https://doi.org/10.1080/07421222.2004.11045797

Zhu, K., Kraemer, K. L., & Xu, S. (2006). The Process of Innovation Assimilation by Firms in Different Countries: A Technology Diffusion Perspective on E-Business. Management Science, 52(10), 1557–1576. https://doi.org/10.1287/mnsc.1050.0487

Zhu, K., Kraemer, K., & Xu, S. (2003). Electronic business adoption by European firms: a cross-country assessment of the facilitators and inhibitors. European Journal of Information Systems, 12(4), 251–268. https://doi.org/10.1057/palgrave.ejis.3000475

Zubair Rafique, M., Van Goethem, T., Joosen, W., Huygens, C., & Nikiforakis, N. (2016). It's Free for a Reason: Exploring the Ecosystem of Free Live Streaming

Services. Proceedings 2016 Network and Distributed System Security Symposium, 1–15. https://doi.org/10.14722/ndss.2016.23030

11. Appendices

Appendix A

00:00:14

Researcher: Hello. My name is Aigerim and first of all, thank you very much for your time and for agreeing to answer my questions.

00:00:44

Thomas Heldrup: No worries, it sounds like an interesting project that you're working on.

00:00:48

Researcher: Thank you so much. If you don't mind, this interview will be recorded and transcribed in the future for my project.

00:00:59

Thomas Heldrup: OK. Oh, that's fine. OK, if you decide to put something from our conversation into your project, please, send it to me first, so I can just say go ahead.

00:01:18

Researcher: It sounds perfect. OK, and let me introduce myself. My name is Aigerim and I'm a graduate student from Aalborg University. I'm conducting a research on the

fight against the illegal distribution of sports streaming content using a combination of legal tools and artificial intelligence. And I've prepared some questions. If you don't mind, we will begin this conversation.

00:01:50

Thomas Heldrup: Sure. Yeah. Can I just ask what sorts of studies? What are you studying?

00:01:56

Researcher: I'm studying digital communication leadership at Aalborg University. Yeah, I'm doing my Erasmus program. I started my education in Salzburg and then I came to Denmark to continue my studies.

00:02:15

Thomas Heldrup: OK, so you have no legal or technical background or communication?

00:02:23

Researcher: Before I started this Masters, I was working as a project manager in IT companies for four years. We were building software for different organizations.

00:02:36

Thomas Heldrup: OK.

00:02:38

Researcher: So the first question is, could you please tell me what's your position in this organization?

00:02:47

Thomas Heldrup: Sure. So I am. My title is Legal Data Intelligence. So I have a law degree and then in Danish Rights Alliance, I am in charge of the team who are looking at data for our different projects and also doing the legal work in our cases. And I don't know how much you know about the Danish Rights Alliance?

00:03:23

Researcher: Yeah. I visited your website and I read articles.

00:03:28

Thomas Heldrup: Yeah. Because it's still only in Danish, our website and very soon we will publish it in English as well. We just recently updated the site, so I don't know when you looked at it.

00:03:48

Researcher: I have a special tool that translates everything.

00:03:54

Thomas Heldrup: So you've looked at the website recently.

00:03:58

Researcher: Yes. I started looking at your website maybe two months ago when I started this research.

00:04:06

Thomas Heldrup: All right. So I think I think the new website was at that point. But I'm not sure. Please, check if there's a new website because it's been pretty bad and there's a

lot more information about how we work and what we work at. So, you might know this, but we're an interest organization, so we're a non-profit organization with members throughout the creative industries here in Denmark. So it's the music industry, the publishing industry. At the moment, we don't have sports rights as primary members but we're working on that. But what we have done a collaboration with the Spanish Football League La Liga, where we actually have an ongoing and website blocking with them, where we are asking the Danish courts to block the websites of illegal streaming websites that are showing the La Liga, Premier League, Dutch League, all the big football leagues and all kinds of sporting events. So that's our exposure to sports rights. Just so you understand, then, that this is something that we very recently started. It was last year and we started this collaboration with La Liga and the blocking because a positive blocking case. Have you ever seen this case or do you know about these cases?

00:06:25

Researcher: I read that you started already blocking legal streaming platforms

00:06:34

Thomas Heldrup: You know that we have the decisions, the court decisions in English translated versions. If you want to look at those, I can send you them.

00:06:50

Researcher: Thank you.

00:06:51

Thomas Heldrup: Yeah. And so we got the district court, positive reaction from them and we're actually now waiting for the high court, the Eastern High Court, to come with a decision on this case next Wednesday. So the first of July. And so that's pretty interesting because it's the first of its kind here in Denmark protecting sports rights in

this way. And we are arguing that the production of football matches is a creative work and it has to be protected by copyright.

00:07:36

Researcher: Yes, you are right. And I also read that this kind of sport content, it's not a creative content, actually and you cannot use copyright against this kind of illegal activity.

00:07:54

Thomas Heldrup: Traditionally or at least in the legal discourse, it has been questioned whether or not sporting events could be protected by copyright because it's, you know, it's players and the whole game is dictated by rules. And it means you can argue that there's no room for anything creative in that. But what we are arguing is that in the production of the football matches, there is a creative aspect there because there's so many cameras in the stadium and the production team can also apply logos and graphics and sound. And they come from all the different camera angles. They can tell a story that they want depending on if it's two rival teams or one player who was especially well known. Yeah. So that's something quite new in Denmark. And that's going to be very interesting to see if the court wants to go along on that.

00:09:19

Researcher: I have prepared questions. So the Article 17 of EU Copyright Directive says that streaming service providers are required to make their best efforts in order to ensure the unavailability of illegal content. And my question is, are there any, like, laws that take actions against illegal streaming service providers?

00:09:48

Thomas Heldrup: Yeah . So the new directive, Article 17, that's not covering purely illegal services. So that falls back on the current InfoSoc directive. I think it's the InfoSoc Directive from 2001. And there it's this Article 32 which says that you may not communicate to the public protected works. So that's what we are also using in our cases right now, we are blocking the illegal streaming sites. That's it's those articles and the Danish implementations of those articles in Denmark it is the copyright law paragraph two, section three, conferring section four one.

00:10:55

Researcher: So which organizations are involved in preventing the distribution of illegal content, like from a technical point of view.

00:11:17

Thomas Heldrup: So, we use our own infrastructure. That's part of the evidence gathering. And we also have worked together with the La liga. La liga has a big team. I think there are 20 people in this antipiracy technical team where they are monitoring all different kinds of sites and seeing where La liga matches are. So they have a lot of different techniques. Basically we get information from them saying we know there are matches being shown on these websites and then we go in with our tools and then make screenshots and collect links on those sites to then go to court and say there's this much illegal things going on a given website.

00:12:20

Researcher: When you find this website and then what kind of actions you make? Do you make screenshots and then?

00:12:30

Thomas Heldrup: Yeah. So when we go in on a website and then we look at the index that website is showing, because normally the websites that we are handling, they are linking sites to websites that are streaming the content. So they're collecting a lot of different links either themselves or users are uploading links to the website. And we go in and then we take screenshots of the website and the index, and then we also to extract all the different links so we can go to court and say there are this many infringing links on this Web site. And we also take some screenshots of the third-party websites where the matches are actually streamed from so we can prove the whole chain.

00:13:33

Researcher: OK, as I understood it, it's not your organization which blocks this websites.

00:13:40

Thomas Heldrup: No, no, no, that's true. So we can't do that. Right. We set up and in Denmark instead, we go to court against the ISPs. So an Internet provider and its Internet provider were obliged by the court to then prevent Internet providers' users from accessing the Web sites so they will put DNS block on the Web site. So when the user of the Danish Internet provider tries to go on to a Web site that was blocked, they just won't be able to get onto the website. And instead, they are shown an awareness campaign platform called Share with Care, where we get them together with the Ministry of Culture and the trade body of the Internet providers have made this is a shared platform where we will explain the rights that are to creative works and where they can find the legal content and also some of the consequences of not using legal sources. So there's, of course, there's consequences for the industries and their ability to make new content. But also there are some personal consequences because there's a lot of malware on these streaming sites. So that's also something that users should be aware of when they are there.

00:15:40

Researcher: I think users don't know about this thing.

00:15:43

Thomas Heldrup: Yes, exactly. Yeah. They're not aware of this. They're not aware that it's not free, even though it looks like it's free. They're paying with their personal identity

00:15:57

Researcher: And also commercial organizations also use these platforms.

00:16:06

Thomas Heldrup: There are some studies out there, around 60 percent of ads on sports streaming sites are infected with some kind of malware. It's 50 percent of the ads there.

00:16:30

Researcher: Yes. At the same time it's so easy to recreate these websites, which provides different links to illegal streaming platforms. Are there any special tools that monitor this process. Is there a tool that blocks illegal streams in the process of broadcasting a sporting event?

00:17:00

Thomas Heldrup: So you're completely right. It's very easy to duplicate an illegal side. You just have to just change domain and get the content onto that new domain. And because of that, the website blocking cases that we go to court with, also include mirror sites. So and so the decision says that ISP should block the service, which is currently on a website, but also future websites that provide the same content for the same service, which we Danish right alliance provide to the Internet providers. So once a blocked

website starts popping up on you websites, we can tell the ISPs that there are now these new sites and they should block them. And that's. And the outside court, so we simply want someone we deliver a new list of websites that they should block in order to try and prevent these new sites to gain interaction and new users.

00:18:18

Researcher: But it sounds like a never ending story. One months , you provide the list of websites and next month there are new websites and so on.

00:18:31

Thomas Heldrup: So that's one part. Right. And then there are also criminal cases brought against the people behind these cases as well to try and really stop them. And, you know, if it was true, you were never going to prevent everything from being put on the Internet illegaly. But we can do it as difficult as possible for the user. So the user doesn't want to spend a lot of time trying to find new websites that they can use to see illegal content and therefore use the legal content because it's become so difficult to use the legal content. And also, hopefully they will understand at some point that there are consequences for using illegal content. And there's a lot of legal options out there. So, you're completely right. It is a long battle. We're just and it's never going to end, right? Because there's always going to be someone who doesn't want to pay the price of content. That's true. But for the big part of the audience who maybe don't know that it's illegal or who just got a link from a friend, then there is a lot of people that can be nudged to use legal content instead.

00:20:07

Researcher: You mentioned that La Liga provides you with the least of these website. And so your organization. Do you know what kind of tools they use for finding this kind of websites now?

00:20:34

Thomas Heldrup: So I don't know specifically how they do it. Mm hmm. But I know that there is a lot of different ways, right. To find illegal content. You can both do some keyword searches on search engines like Google. And then you can kind of gather a list of different websites and then you can have some technical tools to check, you can watermark some content. And then you can check that watermark up against what you're finding on an illegal platform. And then you can say, OK, here I am with someone showing illegal matches. But it's a complicated process and I don't know specifically, but I would recommend that you maybe try and ask La Liga or some of these other big sports organizations, because they all have dedicated teams doing this. There are also independent companies called antipiracy vendors who are providing this kind of tool to search a lot of different websites for content that's been watermarked on Facebook also. Do you know Facebook rights management? They also have this tool where content owners, they can upload reference files to a special tool on Facebook and then Facebook searches, everything that's being uploaded to the platform and all the matches. You can then say, OK, I want to block this or I want to monetize it or I want to monitor it. And so they also have some some kind of tool. But I don't know the specific technical ways is working, unfortunately.

00:22:36

Researcher: And my question is, maybe you have contacts from La Liga or from different company.I can maybe send a letter and ask the same questions.

00:22:50

Thomas Heldrup: Sure. Sure I can. I can look what I can.

00:22:58

Researcher: Thank you. Have you heard about the potentials of using artificial intelligence against illegal streaming platforms?

00:23:16

Thomas Heldrup: I think that's again, it's something that you have to talk with someone who's in the technical departments because, sure, there's a lot of possible ways I can think of that artificial intelligence can work here with image recognition and things like that. But again, I'm not that that technical, we don't work with that.

00:23:46

Researcher: So maybe, you know, is there any legislation that regulates the use of technology to combat illegal content?

00:23:57

Thomas Heldrup: So legislation that's governing the use of technology specifically. So what are your thoughts behind this question? So should it be legislation that is preventing rights owners from doing stuff to protect their content.

00:24:36

Researcher: Yeah, I read the Article 17, but there's nothing about measures that right holders can take to prevent the illegal sharing. So I was thinking maybe there's like legislation that regulates the use of technology.

00:25:02

Thomas Heldrup: Yeah, it's nothing really that I can think of at the moment. So now you have quite a lot of ways to protect your content because someone is infringing it

00:25:23

Researcher: So they have the right to choose how to protect their content ?

00:25:31

Thomas Heldrup: Yeah. I can't really think of anything specifically governing the ways of protecting content. It's their proper intellectual property so they can do quite a lot to protect it. So you can put your DRM protection on something so you can't copy it or things like that. There are some regulation around that, but that goes the other way around. So that's not regulation on how a copyright owner can protect its more what you're not allowed to break as a user.

00:26:22

Researcher: OK, and what is the role of telecommunication organisations in this fight against illegal streaming. You mention ISPs.

00:26:41

Thomas Heldrup: Yes, they are the telecommunication companies. So they're the ones who are blocking after we have a court order saying that site is illegal and also the awareness campaign platform to show that's also a platform that we've made in collaboration with the telecommunication companies. So we are also in the fight against illegal content.

00:27:18

Researcher: You mention Share with Care with. I also read about it on your website. I found a report, but everything is in danish. Maybe you have an English version.

00:27:32

Thomas Heldrup: Yeah, I think actually we have an English version of the Share with Care report. Let me also see if I can find that. Could you just follow up email? I can get back to you on that. OK, I'm pretty sure that we have an English version of that report.

00:27:55

Researcher: OK, thank you. So I think we can finish this interview for now you on this question. So do you have any questions for me?

00:28:08

Thomas Heldrup: Yeah, we would very much like to see your project once it's finished, because it sounds very interesting to look at this these ways of combating illegal sports rights. And it is something that Danish Rights Alliance is looking at expanding into.

00:28:40

Researcher: When I finish my project, I will send it to you. Thank you so much for your time!

00:29:29

Thomas Heldrup: You're welcome. We'll keep in touch.

00:29:42

Researcher: Thank you so much. Bye bye.

Appendix B

00:00:01

Werner Strydom: My name is Werner I'm originally from Zimbabwe, but I grew up in Namibia and South Africa, but I've been living in the Netherlands for the last 30 years almost. I am responsible currently for a team inside our company which does advanced technology research and development. So it's basically a group that looks at technology trends and tries to identify the things that are going to be mainstream in three to five years. And then for the ones that are relevant to cybersecurity. So to our company and our customers, we would take those technologies and we explore them, we build concepts. And generally we hand it over into the product teams within our organization. So we just do very early stage R&D and early stage product development, but not end to end product development. The team has a number of data scientists in it. And we sort of act as a center of expertise for data science projects in our company. I think that's the reason why Mike Mulready already connected you with me, is because this team was responsible for building most of the initial buildout of most of the machine learning projects that we have.

00:01:34

Researcher: Okay, thank you. And what is your role within the company? Just for my research. How can I present you?

00:01:43

Werner Strydom: Um, so I head up a small department that's responsible for class technology research.

00:01:52

Researcher: Mm hmm. Okay, great. Thank you. And I found a lot of interesting and useful information and articles and white papers on your website. On your company's website. My project's topic is application of artificial intelligence to fight against illegal streaming sports services, sports specifically. Before I was focusing on music and then I decided to change my topic and now I'm focusing on sports content. And I also found a lot of information about it, uh, solutions that, uh, your company works with to prevent online piracy. So could you please tell me more about this area?

00:03:07

Werner Strydom: I think the Irdeto originally got involved in this area through the Blu ray disc technology. So the technology that used to protect Blu-ray discs that they don't really exist anymore. Nobody buys them anymore. But so we got involved in it in sort of the content antipiracy through the Blu ray disc technology. And we have a unit based in Hollywood, in North Hollywood, which is connected to all of the studios there. And over the years, we developed a service for that industry which attempts to track down illegal streaming and illegal downloading of content. The service is very human-intensive. So what happens is we have Web crawlers and these web crawlers are pointed at certain websites that are known to be involved in distributing illegal content. And then the crawlers collect all of the information that they can find. And then analysts have to look at each link that they find to see what content is this. Is it a movie? Is it a TV series? Is it sports? Then they have to see if it is content that we are responsible for protecting. So they have to look to see who is the broadcaster, because it could be, for example, that a sports event is a popular sports event and it's available on ten different broadcasters at the same time. But we are only being paid by one of those broadcasters. To take down the illegal content, so usually broadcasters put a little logo on one of the corners somewhere. So what the analyst does once, once I find a piece of content, let's say it's a sports content, they first understand what type of sports content is it. OK, this is ice hockey. We're not doing any protection for ice hockey. And this is football. Yes, we're

doing protection for football. Then they look to see what the logo is. If they find a logo of one of the paying customers and then they should take down no notice for that content to the website. So it's very human-intensive. You just get the video stream of the video file. And there's no metadata associated with that file other than the name of the file, which sometimes gives you a hint, but sometimes it's completely wrong as well. Quite often, especially with movies, you will come across a file name for a movie that can be downloaded and the file name will tell you this is Lord of the Rings. But when you download it and then you find out it's something else entirely. The Hobbit or maybe even something completely different. So you can't even trust the file name properly. So in order to automate some of this high human intense activity around analyzing the content, we started looking at using machine learning and image processing specifically to do that. So one of the first things we did was build a little image recognition solution, which, first of all, identifies the logo. Where is the logo on the screen, the broadcaster's logo. And once it's isolated the logo, then it matches it to a database of known logos and then makes a prediction to say it's from CBS and it's Channel seven. So that helps a lot with ads or really ads and they are filtering. So all of the video streams that are recognized with a logo or a customer from us, they know those are the ones that they can process, the other ones they can ignore. So that helps already. Then as a next step, we built a machine learning model that can recognize certain types of sports. So a sports classifier basically is what we did. It was only trained to recognize a small number of sports, but it can distinguish, for example, football from hockey and from tennis. So if you are specifically only interested in protecting, let's say, Premier League, then this classifier will be able to automatically detect which of the video streams of video files contain football type commentary.

00:08:20

Researcher: And I also found an article, I think it was made by representatives of your company and it explains every step.

00:08:30

Werner Strydom: Oh, so you've seen that.

00:08:32

Researcher: Yeah, I read that article. It says that you have four steps there. First is the discovery of rebroadcasts and then gathering data from illegal broadcasts and then analyzing and taking measures.

00:08:51

Werner Strydom: So the gathering data is done with crawlers. That's an automated process. Crawlers given some keywords and it'll go and try and find the links to files and streams that are illegal. And then the next one of the next steps is very human-intensive. And it's those steps that we've been trying to automate. So the first step is just to collect all of the links. Just what are the four steps that I mentioned in the article?

00:09:33

Researcher: Oh, yeah. It is a discovery of illegal rebroadcasts. And then gathering data from the illegal broadcasts. Analyzing data and taking measures against.

00:09:51

Werner Strydom: Yep. So taking measures is takedown notices and investigations. But the discovery and gathering data is done with Web crawlers and the web crawlers are geared with some keywords and profiles of certain websites and to be able to collect information. It's the analyzing part where machine learning is used. So basically it's used to add metadata to the files that have been found to the links that have been found. So

another classifier that we developed was one that detects the language that is in the video stream. So once you detect the language, then you can add that little bit of metadata. Once you've detected the logo, you can add that metadata. If you've used a sports classifier and it detects a sport that it recognizes at that metadata and that just makes the work of it filters out a lot of content that the analyses don't have to look at. And so it narrows down because we can collect much, much more data than the analyses can ever look at. We can know that the volume of data out there is thousands of times bigger than our capacity to look at it.

00:11:25

Researcher: And as I also found in that article, you apply the Convolutional Neural Network for image recognition.

00:11:35

Werner Strydom: Yeah, yeah. That's a very standard approach for all of the image recognition stuff. So for sports except for language detection, for example. Um, most of the Life-Support stuff is image recognition. Mm hmm.

00:11:50

Researcher: And my next question, what kind of additional technologies or resources are required in order to be able to adopt your solution ?

00:12:03

Werner Strydom: OK, so we do offer the solution as a service. We don't sell technology. But in order to offer the service, we make use of it. So Web crawler technology, that's one. There's lots of frameworks that you can use to make it easier to find information on the Internet. And a very common one to use is Selenium, I think. Yeah, I think that's the

name selenium, the Selenium framework. And you can easily build web crawlers with that.

00:12:34

Researcher: What is the selenium?

00:12:36

Werner Strydom: And let me just put it that, that I've got the correct name here. It's called Selenium, and what it does is it's a library with functions that you can quickly put together a small program that can look at the content of a website, go through all of the information, all of the links on a website, and by using keywords, filter out certain bits of information that you need. Selenium is like a library that you can use to build these little web crawlers with. Selenium is open source, but the web crawler that we built is our solution. And the web crawler is specific to each website. Because the way let's say and also it's not just websites, it's also, um. Well, I guess it's the website, but it's social media sites like Twitter and Reddit and Facebook, because a lot of information that we're looking for on those websites, each one of these websites has a different layout in a different structure. And so you have to adjust the crawler to the to match how the website works. So that's one technology that you use because of the volume of information that's out there. The solution tends to be implemented in cloud technology like Amazon Web Services, especially since the amount of computing power. If you have 10000 crawlers going out and quickly searching for information, then you need a huge amount of computing power, but you only need it for a short period of time. So making use of Amazon for that is good. It's also very handy because one of the data that it finds and copies that ingestible data into Amazon is free. So you have to pay for the computing power in Aiwass. So that's a second technology that we use. And another technology that we use is to mask who we are because if we just used a data, corporate servers to do the web crawling, then the pirates will quickly detect this with colors

coming from that domain and just block it. So what we have to do is we have to use very large pools of IP addresses and use IP addresses for a short period of time and then discard it. So there's a lot of, not a lot, but there's a bit of technology that we use around keeping our access anonymous so that we can't be blocked by pushing.

00:15:51

Researcher: At the same time, it's really easy to create these illegal websites that provide links to legal content. And what do you think about the effectiveness of application of your solution to detect these illegal services?

00:16:13

Werner Strydom: So you're right, of course they can they can just create a new website. The problem is, if they create a new website, then their customers can't find them easily. So that already if we can shut down one website and have to move to another one, then it slows down the piracy because the customers are used to going to this website and now this website doesn't exist anymore. So that already helps. But of course the crawling of websites is also an automated function. And so we can also very quickly switch from one website to another website. So it is a cat and mouse game for sure. The real problem is not in finding where the illegal content is, because they're almost running it like a business. So they must advertise their products. And if they're advertising the products, we can find them very easily because the customers must be able to find the pirate and the people who are taking the pirate content must be able to find them. The real problem is in getting the cooperation of a species to shut down websites.

00:17:31

Researcher: Mm hmm. But why do you think that it's a problem?

00:17:35

Werner Strydom: Um, it's not generally in the ISPs best interest to shut down websites. They don't really care what their customers are doing, what they care. So the services that they're offering to their customers and if they're running a website that's showing illegal content or they're running a Web shop and the ISP doesn't care and they still get their money. Now, in many countries, there is legislation which makes it possible to issues things like takedown notices, which requires a website then to comply with the takedown. Of course, you have to be very sure that when you do, you should take down notice that it's legitimate. That's why it's important to have a human in this. Look, you can't automate completely and take the human out, because if you issue or takedown notice and it was a mistake, then the ISP will lose trust and they will no longer respond to your takedown notices. So it's very important to build that trust with the ISPs and then, of course, the legal jurisdiction in some countries. It's easy to do this. In other countries, there's just no hope. I mean, if you can't, you should take no notice in Russia or in China and expect that it will be adhered to, that that just doesn't happen.

00:19:34

Researcher: I understand, it's your company's solution. And you should get money from this solution. How do you sell or what kind of companies you work with?

00:19:50

Werner Strydom: So in the sports field, we work with the sports rights holders. So that will be typically somebody like Formula One or the Premier League. It's the organizations that hold the rights to that content. Those organizations are not usually the ones who sell the content directly to the consumer. They sell the content to a broadcaster and the broadcaster sells it to the consumer, although we are beginning to see much more direct selling as well, where it goes directly from Formula One to a to the consumer. So you have the sports rights holder and you have the operator and our customer is the operator. So they pay us to do the takedown and to do the antipiracy

prevention. But we have to work very closely with the rights holders because we're actually exercising the rights that they hold in order to block the content with ISPs who also work with ISPs. But they're not our customers. So we know that we just one of the mechanisms of stopping the illegal content is, is to, is to ask the ISP to cooperate with taking down the content.

00:21:16

Researcher: As I know in Denmark they have Danish Rights Alliance, they work with La Liga and La Liga every month, provide the list of illegal websites. And then, the Danish Rights Alliance sends this list to ISPs and ISPs block these websites, but they have to do it once a month. And I'm not sure that it's quite effective, you know, it takes a couple of days for them to change a website's name.

00:21:52

Werner Strydom: No, no. So our service is also very much geared towards live streaming. And so what we do is 15 minutes before a big game, then we will issue the takedown notices. So then you disrupt or even worse and 15 minutes after the start of the game, because what happens now is if you pay a pirate to get access to illegal broadcast and illegal sportsbook broadcast and 15 minutes into the game, suddenly the broadcast stops, then you will be angry with the pirate that sold it to you so that that also destroys their business model if you do it that way.

00:22:40

Researcher: Mm hmm. So it takes 15 minutes or less to detect these illegal websites?

00:22:46

Werner Strydom: Oh, yes. Yes. Typically in five to ten minutes, we can find the illegal streams. And then it's a matter of getting the cooperation of the ISP to stop it.

00:23:00

Researcher: Mm hmm. Is the competition in your sector high? Do you have competitors?

00:23:10

Werner Strydom: We certainly have competitors. There are some companies, some well-known companies that have been in the media industry for many years providing protection and maybe there's , you know, 10, 20 companies in the world that really are well known for doing this type of activity. It's not like hundreds of thousands of companies that do it. We can't charge a lot of money for this service. It's not an expensive service because if we charge too much, they can still go to another company.

00:24:00

Researcher: And could you provide me with some numbers? With how many companies are you working? I need empirical data for my research. Just to prove that this solution is working and is helping industry to prevent the spread of illegal streaming.

00:24:18

Werner Strydom: OK, so can you give me an idea for what type of empirical data you're looking at? Might not be able to provide all of it, but I will see what information I can gather.

00:24:33

Researcher: How the solution is helping in the industry to prevent the spread of illegal streaming services? What kind of industries and organizations you are working with? Just to show that there are customers, like clients using your solution that is effective.

00:25:00

Werner Strydom: Yeah, I could maybe give you an idea of the number of events that we target, how many sports broadcasts we going to be great. And also the number of organizations with whom we work that make use of our service.

00:25:29

Researcher: Thank you. So you mentioned that your solutions are not so expensive. I just wanted to ask you what kind of organizations can afford your solution?

00:25:42

Werner Strydom: So, um, every single broadcaster can easily afford the solution that it's not a very high cost. We're not talking about thousands of dollars, not hundreds of thousands of dollars. So but what they need to do is they need to weigh it against the benefit they get from it. And that's always a very difficult calculation to do. So if you have a sports event and you don't do anything to protect the illegal broadcast, what is the impact on the sport, on the broadcaster? Will they get one per cent more viewers? Will they get 10 per cent more viewers? And it's almost impossible to determine that because you almost need a time machine where you say and will look at the sports event and we will have no antipiracy services with it. And then we'll go back in time and we'll look at the same sports of it. But this time will do it with antipiracy services. Then you can do a comparison, but you can never really know for sure what the impact is. So there are different ways of doing the calculation, but that's usually done by the operator themselves. So what we can see is that for high profile events like big games, La Liga,

Premier League, the Formula One races, certainly that's worth it. But for local soccer teams, for, you know, for less popular sporting events, it's not worth the trouble.

00:27:37

Researcher: OK, and in terms of legislation, are there any obstacles that can affect the adoption of your solution within the company?

00:27:48

Werner Strydom: A lack of legislation is a problem. While back, even in Scandinavia, there were a lot of piracy because the legislation and the legislation didn't make it illegal for people to watch pirated content. It made it illegal to make pirated content available. But as a consumer, it was fine if you accessed pirated content. And but we are seeing more and more countries introduce legislation to make it illegal to access pirated content and also legislation around takedown notices and blacklisting and ISPs. And that can be a hurdle in terms of existing legislation. That can be a problem. You have to be careful with privacy information. So GDPR, our legislation, you need to be very aware of that and make sure that you don't do anything that contravenes the copyright laws. I think it also depends where you go in some countries, there is legislation around digital rights. Other countries don't have that at all. You know, sometimes in some developing countries, the laws for digital assets haven't been developed yet.

00:29:33

Researcher: OK, thank you. And what do you think about the users of illegal platforms, streaming platforms? Is it possible to change their behavior and convince them to pay for content?

00:29:54

Werner Strydom: I think so. I think it's a combination of making content easily accessible and. But making content, making legal content easily accessible and at a reasonable price and making illegal content difficult to access, I don't think you will ever stop it. But most people, if they're given the option, you could there's a really easy way, the content that you're looking for. There's a really easy way to get access to it. It's not going to cost you a lot of money. Then they would choose that option. But very often you find that and this is with sports quite often the case, especially with people who live in a different country from where they were born and they can't access the sport from their home country because it's not available in their own country. So the only option they have is, is to go for illegal streaming. So that's very understandable. It's illegal. So you have to be careful. You shouldn't do that. But, yeah, it's understandable that people actually do that. But we're where I think I have no sympathy is if you're able to afford the content and you're not not paying for it, then you're actually destroying the future of that sport with that content. Right. If all of the Disney content was pirated and nobody paid for it, then Disney will stop making content and the sports teams will stop being able to afford good players.

00:01:45

Researcher: And, um, you're right.

00:01:48

Werner Strydom: But I don't think you can change everybody's mind. There's always a core group of people who just seem not to be interested in doing things the right way. But there is always a group of people that you just need to put a little bit of effort into to keep them honest. And they will and they will stay honest.

00:02:11

Researcher: OK, thank you. What do you think about the decision-making process within the industry? Is it easy to come to accept your solution, adopt your solution for industry? Right. If you understand my question.

00:02:39

Werner Strydom: It is really easy to make use of the service and broadcast. It doesn't have to do any effort to make it work. They just need to reach out to us and we can provide the service also. They know where to go to. We're very well known in the industry and our competitors are very well known in the industry. So if you're a broadcaster and you think I need to protect this sports broadcast, then they know exactly where to go. So it's easily accessible to the industry. I don't think there are hurdles with access to service.Does that answer the question?

00:03:20

Researcher: Yes. Yes. You answered my question. Thank you so much. And I think it was my last question. But if you want to add something.

00:03:37

Werner Strydom: Yeah, I could maybe you probably accessed all of the publicly available information. I'll see if there's maybe a little bit more information around me and how we use it in sports broadcast. And if I find anything, I will share that with you. Great. Thank you. I know I will get back to you on some stats that we finish.

00:04:01

Researcher: Great. Thank you so much for this interesting conversation. And yeah, it was really interesting and useful for my research and for me.

00:04:09

Werner Strydom: OK, so what do you do with this information?

00:04:17

Researcher: I'm going to transcribe our audio and then I will analyze it and present it in my thesis.

00:04:25

Werner Strydom: OK. Are you speaking to more people?

00:04:28

Researcher: Uh, yes, I already had an interview with an expert from the Danish Rights Alliance.

00:04:41

Werner Strydom: OK, so that's good.

00:04:45

Researcher: Because I'm not focusing only on A.I. as a solution, but like, um, uh, I want to analyze how not only A.I., but also legal tools can work together to prevent.

00:05:05

Werner Strydom: What I will add as additional information is that, um, quite often people think of machine learning as a threat, something that will destroy jobs or things like that. But in this instance, it's definitely not the case. Without AI, we can only look at a small amount of data, um, with the analysts that we have. So we have 100 analysts. They can only monitor so many websites and so many illegal video streams with those people. AI makes it possible for them to look at a larger website. It's not that we have

fewer analysts working on the job. It's just enabling. It's empowering them. It's human augmentation, not human replacement.

00:05:53

Researcher: Mm hmm. But I also read that in order to be able to use machine learning , you need to train it.

00:06:04

Werner Strydom: So it takes a lot of data and it does, but there is the good and that's always a problem with many AI implementations, is that people can identify, oh, I will work very well here to do this job. But then they can't find the data to train the model. Unfortunately, in our case, there is more data than we can ever use. And we've been doing this for you know, we've been calling for many years. And so the amount of data that's available to train A.I. is huge. It's relatively easy to do it.

00:06:43

Researcher: Mm hmm. OK, thank you so much.

00:06:47

Werner Strydom: OK, good luck.

00:06:51

Researcher: And I will wait for your email. Thank you so much. Have a good day.

00:06:57

Werner Strydom: You too. Bye.