Technological solution‘s feasibility study regarding restricting access to illegal content on the Internet

Summary

Intended for: Ministry of Culture of the Republic of Lithuania

Vilnius, 2025

LIETUVOS RESPUBLIKOS KULTŪROS MINISTERIJA

Smart Continent

CONTENTS

INTRODUCTION

Smart Continent management Institute, UAB, in accordance with Agreement No. VP-289 signed on December 10, 2024, with the Ministry of Culture of the Republic of Lithuania, it is preparing a feasibility study and its appendix (hereinafter referred to as the Study) on a technological solution to restrict access to illegal content on the Internet. This summary of the Study in Lithuanian has been prepared in accordance with the requirements set out in the annex to the agreement – the technical specifications (hereinafter referred to as the Technical Specifications or TS).

STUDY ASSUMPTIONS: According to data from a 2021 study by the European Union Intellectual Property Office (EUIPO), Lithuania ranks third among all European Union (EU) countries in terms of the consumption of illegal content that infringes on the rights of copyright holders. On average, internet users in Lithuania access illegal content about 12 times per month, while the EU average is only 5.9 times. According to the 2019 study, the average Lithuanian internet user accessed pirated websites almost 26 times per month, while the EU average was 9.7 visits per month per average user. Based on ESINT studies, it can be observed that Lithuania has remained one of the most pirated countries in the EU for several years in a row. In the latest ESINT 2023 study, Lithuania, together with Latvia, Estonia, and Cyprus, is again ranked among the EU member states with the highest levels of content piracy.

Given the current situation, it can be concluded that a significant proportion of audiovisual content users are simply unaware that they are consuming illegal content. A study to determine the level of illegal content consumption among Lithuanian residents was initiated by the Ministry of Culture in 2023. As many as 20–25% of content users indicated that they were unable to distinguish between legal and illegal content access. Therefore, there is currently a need for an innovative technological solution that would enable honest audiovisual content users to verify the legality of the content they consume, direct them to legal content sources, and enable state institutions to monitor the distribution of illegal content. After conducting a market consultation on the development of such a technological solution, it became clear that modern innovative technologies offer a variety of ways to achieve the above objectives, so it was decided to purchase feasibility study services.

According to the provisions of the Ministry of Culture, the objectives of the Ministry of Culture include, among other things, shaping state policy in the areas of copyright, performers and other related rights, and public information (audiovisual policy is an integral part of public information policy), as well as organizing, coordinating, and controlling its implementation. Efforts will be made to positively shape legal content consumption habits by helping users not only to identify pirated content, but also to find legal sources of similar content.

STUDY'S AIM:

1. based on an analysis of piracy in the audiovisual services market and user needs, an analysis of best practices in other countries and existing technological solutions on the market and their application methods, select the most effective technological solution according to your chosen criteria.
2. provide a description of the structure of the alternative technological solution selected by the contracting authority, a cost-benefit analysis, and implementation methods, detailing each of them in accordance with the parameters set out in this technical specification (i.e., prepare the technical specification of the technological solution).

OBJECTIVES OF THE ANALYSIS AND METHODOLOGY

It should be noted that "alternative" in the context of a technological solution, given the expanded concept of a technological solution, can be understood in different ways. The following describes different concepts for formulating alternatives:

- Concept (problems to be solved) – considering the expanded concept of a technological solution, different concepts of a technological solution are possible. Different concepts can solve different problems (single or multiple) related to the distribution and use of illegal content.
- Functional parts – possible concepts of technological solutions, where more than one problem is being solved, a technological solution may have different functional parts. For example, functional part A is designed to detect illegal content and technological part B is designed to offer a legal source. This distinction is important because the same functional parts can be combined in different ways.
- Technology (functional part implementation) options – the same functional part can be implemented using different technologies. For example, the functional part of detecting illegal content can be implemented by comparing website data with lists of websites distributing illegal content in a database (simple comparison algorithms) or by applying AI to analyze website characteristics. Each of the different technologies that can be used to implement the functional part is called a technology variant.
- Technological solution alternative – a technological solution alternative is a solution that combines the concept (problems to be solved), functional parts, and technology (implementation of functional parts) variants. Considering that the technological solution may be improved and further developed in the future (after the implementation of the first version), possible additional functional parts are envisaged for each technological solution alternative.

The concepts described above are developed in the following ways:

- Possible concepts (problems to be solved) are developed based on the identified problems, according to how existing or possible solutions solve such or similar problems. Problems and their possible solutions (according to expert assessment) are identified by analyzing expert opinions. During this analysis, the problems and possible solutions expressed by the experts are grouped and combined into problem-cause-solution (intervention logic) diagrams. Different intervention logics are formulated into different concepts. The concepts are validated by comparing them with the concepts of existing solutions.
- Functional parts are determined based on an analysis of the elements necessary for the implementation of the concept. When analyzing the elements of concepts, functionally separate, directly unrelated parts of concepts are identified. If identical functional parts are required to implement different concepts, they are combined.
- Technology (functional part implementation) options are identified based on an analysis of the technologies used in existing solutions and an analysis of expert interview material.
- Technological solution alternatives are developed considering logically possible alternatives for the implementation of concepts (combinations of concepts, functional parts, and technological variants).

The figure below presents a diagram visualizing the methodology of the study.

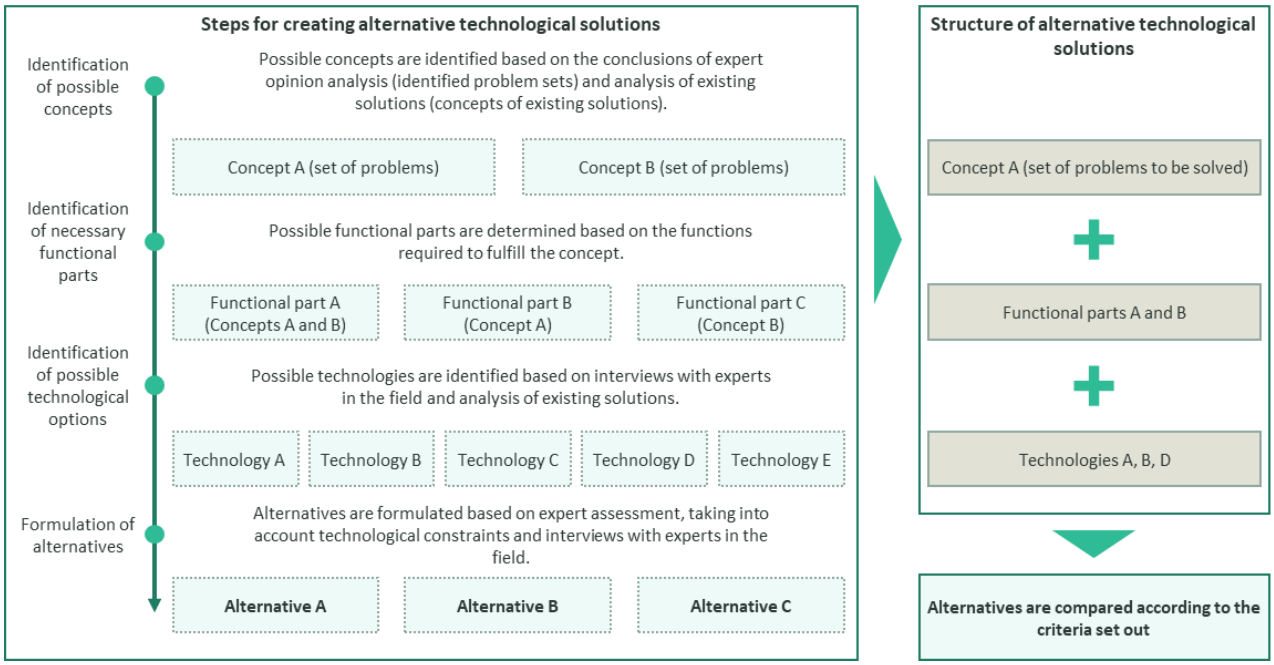

Figure 1. Studies' I stage methodology visualization diagram
Source: prepared by Consultant

Descriptions of possible developments are drawn up for the alternatives that have been identified. These descriptions highlight the functional parts that are not necessary for the implementation of the alternative and that could be implemented in the future, once it has been established that the implemented solution effectively implements the concept of the solution. Development descriptions are prepared based on an analysis of the applicability of the functional parts of other alternatives to the alternative. The functional parts of other alternatives that could be applied to the concept of the alternative are included in the description of the alternative's development.

The alternatives developed are compared according to the criteria set. The following comparison criteria are set:

- Complexity, risk of technological failure – the level of novelty/innovation of technological implementation is determined. The assessment is made by applying one of the following characteristics: a) "Uncomplicated" – this assessment is assigned to alternatives that use widely available technologies for implementation; b) "Complex" – this rating is assigned to alternatives that require the use of technologies that are not widely used and require the expertise of rare and advanced ICT specialists; c) "Innovative" – this rating is assigned to alternatives whose implementation would require the application of advanced technologies, i.e., there is no existing application of any of the technologies under consideration to achieve a similar concept.
- Initial investment – the relative size of the initial investment is determined based on available market prices. The size of the investment is indicated in nominal reference values, with a more favorable assessment being assigned to alternatives with lower costs.
- Complexity of maintenance, maintenance costs – the assessment is based on two components: the expected costs of maintaining connections with external systems and the expected human resource costs. A more favorable assessment is given to alternatives with lower maintenance costs.
- User experience – the assessment is based on the expected user experience when using the alternative technological solution. Given that different alternatives may vary significantly, a separate assessment is carried out for each alternative to justify the assessment.

Depending on the specifics of the alternatives, additional criteria may be applied.

TECHNOLOGICAL SOLUTIONS’ INTEGRATION AND USAGE IN FOREIGN COUNTRIES

The study presents versions of technological solutions that have already been implemented in foreign countries. The following solutions, which are used in practice, are presented:

- Digital Services Act (hereinafter referred to as DSA) – performs independent reporting of users to services and a blocking function. The DSA provides for a multi-level system of obligations for intermediary service providers. This means that, in addition to the general obligations applicable to all intermediary services, certain types of intermediary services are subject to additional or specific obligations;
- Lumière tool (Spanish case) – performs information identification and blocking functions. The use of this tool helps to investigate intellectual property rights infringements more effectively and optimize enforcement processes;
- “Google” Safe Browsing – performs information identification and notification functions. Safe browsing protection measures are implemented in all Google products and ensure safer browsing across the entire internet;
- EOL tool (French case) – performs information detection, reporting, and legal content alternative suggestion functions. On January 1, 2022, a new law came into force in France, and Arcom, the institution that supervises and manages this tool, was established. – stricter than the previous copyright protection law No feedback on the effectiveness of this tool has been found in the public online space, probably because the tool is relatively new and not yet widely used. Only 14 users have downloaded the Mozilla Firefox browser version of the plugin. The main problem with the plugin is its low coverage rate, which means that in most cases, the plugin does not know whether the website visited is legal or not.
- JustWatch platform – offers alternatives for legal content. The goal is to help users find legal audiovisual content broadcast on legal platforms more quickly.
- Lithuanian analogues: Use Legally, created by the E-culture platform; in Europe: Agorateka.
- Oxylab solutions – performs information detection. An IT tool operating in the Lithuanian market that uses AI technology to detect harmful content on the internet.
- Teramind – performs information detection. This is a platform designed for analyzing the behavior of users who have installed the Teramind program, tracking employees, and reducing internal risks.

Analyzing the application of technological solutions in foreign countries allowed us to examine how similar technological solutions work in practice, as well as the nuances and obstacles of their operation.

ANALYSIS OF EXPERTS OPINIONS

During the consultation process with interested parties, 10 interviews were conducted (some respondents provided written responses). A total of 15 individuals (hereinafter referred to as experts) participated in the interviews. The experts' qualifications are based on the fact that they were delegated by organizations working in areas related to the problem of illegal content. Accordingly, it is considered that the organizations that delegated the individuals (experts) appointed their representatives based on their competencies.

When asked to name the most common technological piracy models that cause the most problems for Lithuanian creators, through which illegal content reaches the user and, conversely, the user reaches illegal content, the respondents named the following:

- illegally broadcast content on a website;
- peer-to-peer technologies;
- downloading illegal content to one's device from a website;

- illegal copying of legal content.

Approximately half of the respondents stated that one of the most important ways to effectively combat piracy is prevention through education. The most effective way to combat piracy was mentioned as informing the public / attention-grabbing warnings to individuals attempting to consume illegal content (the inevitability of punishment).

Respondents' opinions on the effectiveness of penalties in combating online piracy varied. Some respondents said that fines are an effective way to combat online piracy and that both users and distributors should be punished. Others argued that users of illegal content should be punished first and were skeptical of users who claimed they did not know that they were consuming illegal content. A third group said that users have the least influence on the spread of illegal content online, as they are not responsible for its distribution, and therefore stricter penalties should be aimed at those who upload illegal content to the internet.

Almost all respondents emphasized that blocking websites that host illegal content would yield the fastest and most effective results and that this should be a key tool in the fight against illegal content. The diagram below shows the links between the problems identified, their causes, and possible solutions (see figure below).

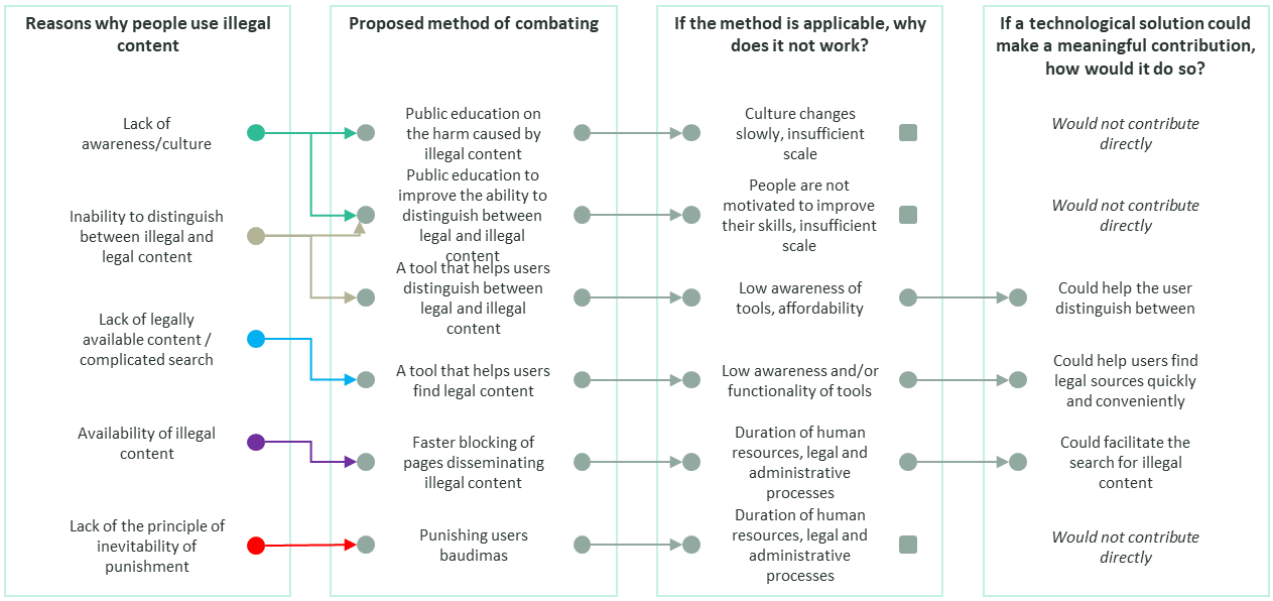

Figure 2. A diagram of problems, causes, and possible solutions based on expert opinions
Source: prepared by Consultant

Accordingly, several groups of problems and solutions can be identified that could form the basis for the concepts of the technological solution being developed:

- Some members of society find it difficult to distinguish between legal and illegal content; the technological solution being developed could help such individuals to distinguish between legal and illegal content;
- Part of society finds it difficult to find legal sources of content, which are related to the fragmentation of legal sources (there are many legal sources, but the desired content may only be available in one of them);
- One of the reasons why the process of blocking websites hosting illegal content is slow is that identifying and monitoring them requires many human resources, as websites with such content are multiplying rapidly;

These groups of problems are used to form concepts.

POSSIBLE CONCEPTS AND THEIR FUNCTIONAL PARTS

Based on the problems identified, the following groups of problems can be distinguished for the technological solution being developed:

- First group of problems: some members of society find it difficult to distinguish between legal and illegal content; the technological solution being developed could help such individuals to distinguish between legal and illegal content.
- Second group of problems: part of society finds it difficult to find legal sources of content, partly due to the fragmentation of legal sources (there are many legal sources, but the desired content may only be available in one of them).
- The third group of problems: one of the reasons why the process of blocking websites hosting illegal content is slow is the need for human resources to quickly detect websites hosting illegal content. The technological solution being developed could increase the speed of detection of such websites.

Accordingly, the following concepts are being developed to solve the identified problems:

CONCEPT A: a technological solution that would be able to detect when a user is attempting to view illegal content and inform them. The technological solution should implement the functional parts of detecting illegal content and informing the user. The format of the technological solution could be a program or a browser extension (plug-in). Users would install the technological solution voluntarily. The target audience for the technological solution would be conscious users who find it difficult to distinguish illegal content (older users and users with a generally lower level of knowledge and skills) and public institutions and institutions that administer public access computers (libraries, schools, etc.). Similar solutions include Google Safe Browsing and the EOL plugin.

CONCEPT B: a technological solution that would function as an integrated search tool. The technological solution should implement content search and legal content databases (proprietary and/or linked to existing databases). The format of the technological solution could be a website or a browser extension (plug-in). If the browser extension format is chosen, users would install such an extension voluntarily. The target audience for the technological solution is conscious users who encounter difficulties when searching for illegal content. Similar solutions include JustWatch and Naudoklegaliai.lt.

CONCEPT C: a technological solution that would combine the two concepts described above. The main difference is that such a solution could not operate in the format of a website (as in Concept B) – it would require implementation in the form of a browser plugin or program.

Considering the concepts described above, the following is a list of the necessary functional parts:

- FUNCTIONAL PART I: Recognition of browsing traffic in the user's system. This functional part is necessary for the implementation of concepts A and C. There are different options for implementing this functional part.
- FUNCTIONAL PART II: Detection of illegal content in the user's browsing traffic. This functional part is necessary for the implementation of concepts A and C. There are different options for implementing this functional part.
- FUNCTIONAL PART III: Warning the user about detected illegal content. This functional part is necessary for the implementation of concepts A and C. There are different options for implementing this functional part.
- FUNCTIONAL PART IV: Search for legal sources. This functional part is necessary for the implementation of concepts B and C. There are different options for the implementation of this functional part.
- FUNCTIONAL PART V: Database of legal sources or links to such databases. This functional part is necessary for the implementation of concepts B and C. There are different options for implementing this functional part.
- FUNCTIONAL PART VI: System for reporting potentially illegal content. This functional part is necessary for the implementation of concepts A and C. There are different options for implementing this functional part.

It should be noted that these are only the functional parts necessary for the minimal implementation of the concepts. Once the alternatives have been formed, development descriptions should be prepared. Different

implementation options were considered for each functional part. After the analysis, the most suitable implementation methods were identified, and alternatives were prepared.

FORMULATION OF ALTERNATIVES

For each alternative, the concept of the first version of the technological solution being developed, its functional parts, and technological implementation options are specified. In addition, development opportunities are described – which functional parts and/or technological implementation options could be realized in the future, after verifying the viability of the concept.

ALTERNATIVE A1 – USER ASSISTANT IN THE FORM OF AN APP (WITHOUT ADVANCED ALGORITHMS, BASED ON DATABASES)

Concept A: a technological solution that would be able to detect when a user is attempting to view illegal content and inform them of this. The technological solution should include functional components for detecting illegal content and informing users. The format of the technological solution could be a program or a browser extension (plug-in). Users would install the technological solution voluntarily. The target audience for the technological solution is conscious users who find it difficult to distinguish illegal content (older users and, in general, users with a lower level of knowledge and skills) and public institutions and institutions that administer public access computers (libraries, schools, etc.). Similar solutions include Google Safe Browsing and the EOL plugin.

ALTERNATIVE A2 – USER ASSISTANT IN THE FORM OF A PROGRAM (WITHOUT ADVANCED ALGORITHMS, BASED ON SIMILARITY DETERMINATION)

Concept A: a technological solution that would be able to detect when a user is attempting to view illegal content and inform them. The technological solution should include functional components for detecting illegal content and informing users. The format of the technological solution could be a program or a browser extension (plug-in). Users would install the technological solution voluntarily. The target audience for the technological solution is conscious users who find it difficult to distinguish illegal content (older users and, in general, users with lower levels of knowledge and skills) and public institutions and institutions that administer public access computers (libraries, schools, etc.).

Unlike Alternative A1, not only browsing traffic is evaluated, but all activity on the computer. This requires a program form.

Implementing this alternative would create a program that collects huge amounts of personal data, raising serious doubts about users' willingness to install such a solution.

ALTERNATIVE B – LEGAL CONTENT SOURCE SEARCH ENGINE

Concept B: a technological solution that would function as an integrated search tool. The technological solution should include content search and legal content databases (own and/or links to existing databases). The format of the technological solution could be a website or a browser extension (plug-in). If the browser extension format is chosen, users would install such an extension voluntarily. The target audience for the technological solution is conscious users who encounter difficulties when searching for illegal content. Similar solutions include JustWatch and Naudoklegaliai.lt.

Implementing this alternative would involve creating a version of JustWatch adapted to the Lithuanian market. The alternative can be implemented by significantly expanding the functionality of the Naudoklegaliai.lt website.

ALTERNATIVE C1 – INTEGRATED PLATFORM FOR AVOIDING ILLEGAL CONTENT AND SEARCHING FOR LEGAL CONTENT (PLUGIN FORM)

Concept C: a technological solution that would combine the two concepts described above. The main difference is that such a solution could not operate in the format of a website (as in Concept B) – it would require a browser plug-in or application.

Implementing this alternative would create a hybrid of alternatives A1 and B. On the one hand, this would mean that the technological solution would be more user-friendly and offer a wider range of functions. On the other hand, the costs of implementing and maintaining the technological solution would be higher.

ALTERNATIVE C2 – INTEGRATED PLATFORM FOR AVOIDING ILLEGAL CONTENT AND SEARCHING FOR LEGAL CONTENT (PROGRAM FORM)

Concept C: a technological solution that would combine the two concepts described above. The main difference is that such a solution could not operate in the format of a website (as in Concept B) – it would require a browser plug-in or application.

Implementing this alternative would create a hybrid of alternatives A2 and B. On the one hand, this would mean that the technological solution would be more user-friendly and offer a wider range of functions. On the other hand, the costs of implementing and maintaining the technological solution would be higher.

Implementing this alternative would create a program that collects large amounts of personal data, which raises serious doubts about users' willingness to install such a solution.

The following section compares these alternatives and formulates a proposal for the optimal alternative. It should be noted that the final decision on the chosen alternative is made by the Client.

SELECTION OF THE OPTIMAL TECHNOLOGICAL SOLUTION FOR LITHUANIA

The alternatives developed were compared according to the following criteria

Figure 3. Evaluation and comparison of technological solution alternatives

Evaluation criteria	Alternative A1 "User assistant in the form of a plug-in"	Alternative A2 "User assistant in the form of a program"	Alternative B "Search engine for legal content sources"	Alternative C1 "Integrated platform for avoiding illegal content and searching for legal content (plug-in)"	Alternative C2 "Integrated platform for avoiding illegal content and searching for legal content (program)"
Complexity, risks due to inability to technologically implement	Uncomplicated in the initial stages, but a complex level will be reached as the solution develops (due to AI integration)	Complex	Uncomplicated in the initial stages, but a complex level will be reached as the solution develops (due to AI integration)	Uncomplicated in the initial stages, but a complex level will be reached as the solution develops (due to AI integration)	Complex
Initial investment	Positive (investment of €70,000–120,000), but the necessary investment would increase as the solution is developed	Negative (required investments may exceed EUR 1 million)	Positive (investment of €300, 000), but the necessary investment would increase as the solution is developed	Average (investments up to EUR 500,000), but the necessary investments would increase as the solution is developed	Negative (required investments may exceed EUR 1 million)
Complexity of support, support costs	Low at first, but support costs would increase as functions expanded	Higher maintenance costs due to higher through put	Low at first, but support costs would increase as functions expanded	Average, but would increase as the solution is developed	Higher maintenance costs due to higher through put
Does it help users distinguish illegal content?	Yes	Yes	No	Yes	Yes
Does it help users find legal sources?	No	No	Yes	Yes	Yes
User's experience	Viewed positively, but some users may find it unacceptable to share their browsing history	Negative assessment, as users will need to share a large amount of confidential data with the administering organization	Positive assessment, but depends on implementation	Positive assessment, but depends on implementation	Negative assessment, as users will need to share a large amount of confidential data with the administering organization.

Source: prepared by Consultant

The customer decided to go with option A1, "User assistant in the form of a plugin."

DESCRIPTION OF THE TECHNOLOGICAL SOLUTION AND DEVELOPMENT OPPORTUNITIES

The following is a schematic diagram of the implementation of the selected alternative.

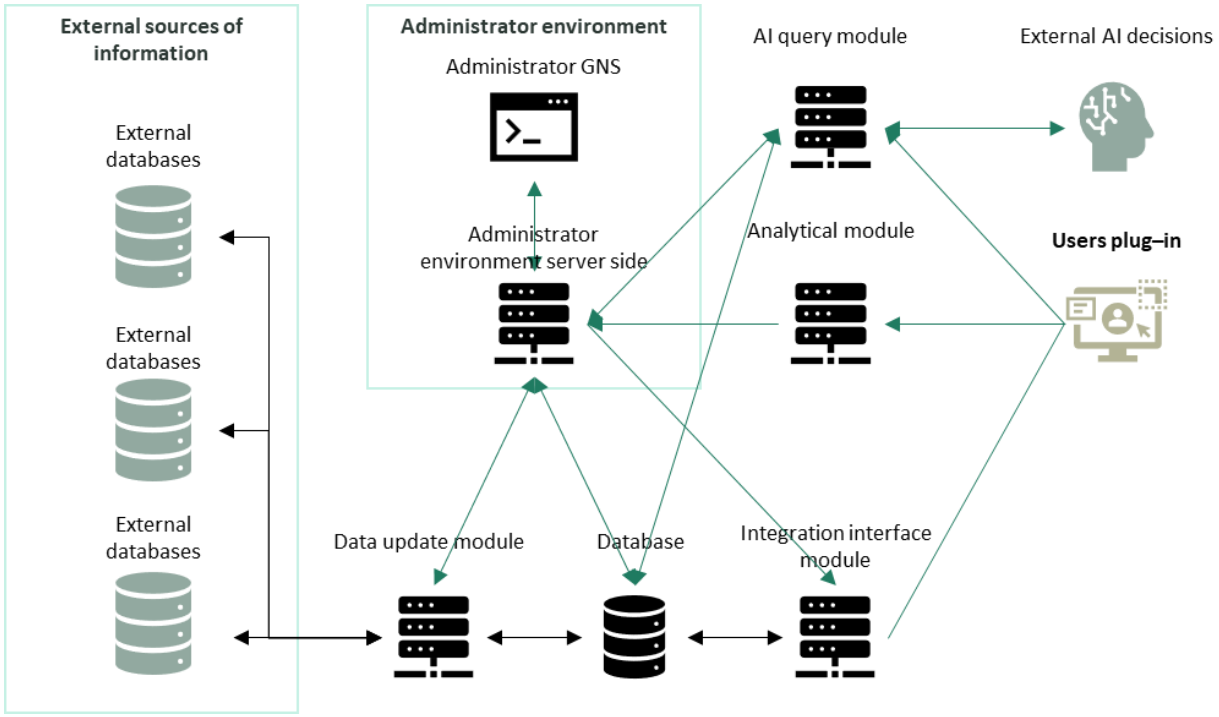

Figure 4. Schematic diagram of the technological solution
Source: prepared by Consultant

The technological solution consists of six main parts, which interact with external databases and AI solutions via a server (see the figure above). It should be noted that external databases are an abstract concept used to describe external sources of information. These parts are:

1. User plugin. A plugin that runs on the user's device. The plugin will search for websites that distribute illegal content;

2. Administrator environment (graphical part of the administrator environment (hereinafter referred to as GNS) and server side of the administrator environment);

3. Integration interface module (responsible for providing information to user plugins and receiving queries from user plugins);

4. Database (stored data, updated from external data sources or manually);

5. Data update module designed to ensure interfaces between the system being developed and external information sources;

6. DI query module designed to ensure integration with external DI systems and to ensure the proper functioning of DI-related functionalities in general.

The comparison of the user's browsing experience with the list of websites distributing illegal and legal content takes place locally, in the user's plug-in. The plug-in compares the hostname of the opened page with the locally stored list. If a match is found, a graphical result (graphical message to the user) is displayed and sent to the analytical module (information about the visited website, the unique code of the user's plugin, and other information specified in the administrator's environment). If there is no entry for such a website in the list of illegal

and legal websites, the user is informed that there is no response and is offered to report the suspicious page or contact the DI.

The automated query DI function is implemented by creating a DI query module on the server side. The purpose of the module is to generate a query to the database containing information about previous queries made by all users to the DI function and the DI responses to those queries upon receiving a user query to the DI. If a query has already been made to the AI platform about the website in the past, the result is returned to the user from the database, and the query is not repeated. It should be noted that, given the development of AI, previous queries may no longer be relevant. For this reason, it is proposed to introduce a limitation period, after which a repeat query to AI would be made upon receipt of a user query, regardless of whether the AI response is stored in the database. In addition, the list of AI responses should be available to the system administrator so that pages for which the AI has given a negative response can be checked manually. If the suspicion is confirmed, information about the detected potentially illegal content should be forwarded to the responsible authorities (primarily the LRTK) for investigation.

Conceptual visualizations of the plugin are presented below.

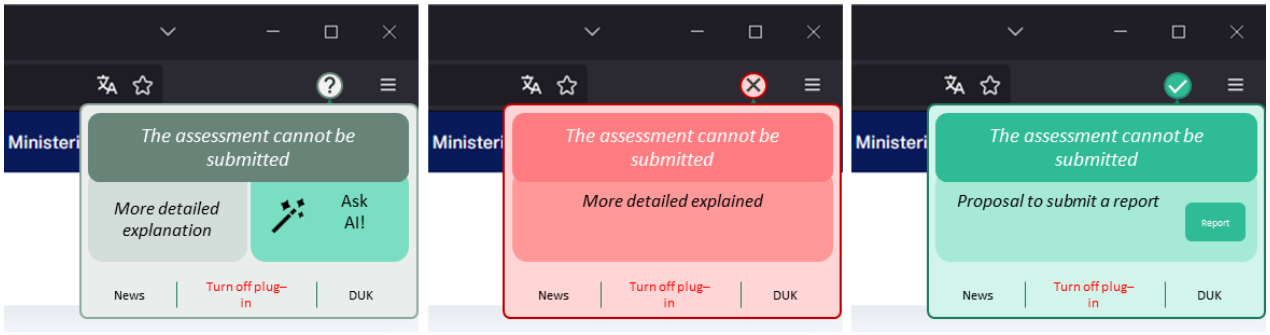

Figure 5. Conceptual visualizations of different scenarios for the plugin. The first image shows a case where the plugin cannot provide an assessment, the second image shows that the plugin has determined that the page is included in the list of illegal websites, and the third image shows that the plugin has determined that the page is included in the list of legal websites.
Source: prepared by Consultant

The management environment establishes links with external systems – both in terms of the frequency and principle of data retrieval and the presentation of information (e.g., a confirmed report of a potentially illegal website).

To ensure the proper implementation of the technological solution, it is necessary to ensure the implementation of the other features described below.

The technological solution, if technically possible, must be compatible with the following platforms:

- It must be ensured that it works in Chrome (as well as in browsers that use the Chrome browser engine and support such plugins) and Firefox browser versions on Windows and Linux platforms;
- It must be compatible with Safari browsers on MacOS, iOS, and iPadOS platforms;
- It must be compatible with Firefox for Android browsers on Android platforms.

These browsers are chosen because of their popularity among users. According to StatCounter Global Stats data for the period 2024–2025, the most popular and frequently used browsers in the Lithuanian region are as follows: Chrome (average 65% of all users), Safari (average 26% of all users), Firefox (average 3.5% of all users). These three browsers cover more than 90% of the market.

DESCRIPTION OF THE PROCESS OF CREATING AND MAINTAINING THE TECHNOLOGICAL

To ensure that the Technological Solution is properly implemented, this section provides a description of the creation and maintenance process and the requirements for the Technological Solution.

The creation and maintenance of the Technological Solution consists of the following stages:

- Stage I. The developers of the Technological Solution (hereinafter referred to as the Service Provider) must agree on the terms and conditions for the development of the prototype with the Contracting Authority, considering the technical specifications of the Technological Solution (see Annex 1);
- Stage II. Service providers prepare a prototype of the technological solution and test it (see Appendix 1);
- Stage III. Service providers should adjust the prototype of the Technological Solution, prepare a version ready for practical operation, and the Technological Solution shall become operational (see Appendix 1);
- Stage IV. The technological solution is monitored, and system updates are performed as needed.

A detailed service level agreement should be prepared in stage III. A summary of the SLA is provided below.

The SLA consists of the following components:

- Response time and reaction to unforeseen circumstances requirements: a commitment to notify users of system malfunctions within 24 hours and to restore system operation within 5 days;
- System availability (operational reliability) requirements: a commitment to ensure that the system will be operational 95% of the time;
- Requirements for notifications of temporary system downtime: notifications of such disruptions are provided to users 5 days in advance;
- Support availability requirements: support is provided to users by email on working days between 9 a.m. and 3 p.m. Requests are responded to within 1 day.

COST-BENEFIT ANALYSIS OF THE TECHNOLOGICAL SOLUTION

The number of users of the technological solution and its change over time will depend on:

- The accuracy of determining the size of the target audience (whether the number of potential users determined in this and other studies is close enough to reality);
- The effectiveness of publicity and marketing activities (whether publicity, marketing companies and activities will be effective);
- The quality of the technological solution;
- The application of administrative measures (whether it will be decided to make the installation of the technological solution on public institution computers mandatory, etc.).

These actions cannot be assessed at this stage, especially as they are subject to change. For this reason, all further actions will be assessed as the expected average of unique users. It is determined as follows:

1. It is likely that the publicity measures for the Technological Solution will reach all members of the target audience, so 100% of the audience will potentially be interested in the Technological Solution;

2. Based on studies of the probability of clicking on advertising messages, up to 13.1% of people who see an advertising message go to the advertised page in the field of art and entertainment. Therefore, it is estimated that there will be 12,800 such people;

3. Based on conversion studies analyzing how many interested people become users, it is estimated that about 5% of interested visitors would become users. In this case, one advertising campaign could attract 579 users – however, it is planned to run such campaigns on a regular basis. A simple audience growth model is presented below.

The model assumes that advertising campaigns will be launched 12 times a year, resulting in 13.1% of clicks on advertising messages (from unique users in the target audience), with 5% of these visitors becoming users. After a year, 30% of users would be retained due to natural user attrition. After another year, the situation would repeat itself.

Given that TS indicates that Lithuania suffers losses of EUR 15 million due to the consumption of illegal content, and this figure is generally lower than other estimates, to safely assess the extent of the losses, it is assumed that the technological solution will reduce losses by 4%, i.e. EUR 600,000 per year from the start of operation. The cost component is presented below.

The cost component consists of:

- Creation costs;
- Publicity costs;
- Server maintenance costs;
- DI service costs;
- Salaries of service personnel.

Adding up the above cost items gives a total annual cost of approximately EUR 77,000 per year.

A standard cost-benefit analysis is performed using a financial discount rate of 4% and a social discount rate of 5%. The analysis period is 15 years.

The following results are obtained after performing a CBA analysis for a period of 15 years:

- Economic net present value (ENPV) – EUR 5,585,359;
- Economic benefit-cost ratio (EBCR) – 8.6. Note – a result greater than one is considered good. This result is considered particularly good.

To summarize the SNA analysis, it can be said that the implementation of the technological solution is beneficial and effective.

TECHNICAL SPECIFICATIONS OF THE TECHNOLOGICAL SOLUTION BEING DEVELOPED

The result of the feasibility study is presented below – Technical Specification of the Technological Solution Being Developed.

1 table. Appendix to the feasibility study – Technical specifications of the technological solution being developed

No.	Requirements
	Functional requirements
FR-1	The purpose of the Technological Solution (hereinafter referred to as TSL) is to conveniently inform the user about potentially illegal content. TSL should be attractive to target groups, and the best visual and technical solutions should be applied for this purpose.
FR-2	The TSL must consist of the functional parts specified in points FR-2.1–FR-2.5:
FR-2.1	a browser plug-in that the user can download and install on supported systems (see Non-functional requirements);

No.	Requirements
	a server side and database for storing TSL data and ensuring the functionality of the browser plug-in (see FR-2.1);
FR-2.2	application programming interfaces (APIs) designed to receive and provide data to external data sources and systems and browser plug-ins (data update module, API module, analytical module;
FR-2.3	application programming interfaces (APIs) designed to receive and provide data to external data sources and systems and browser plug-ins (data update module, API module, analytical module;
FR-2.4	a management environment designed to ensure the work of TSL system administrators;
FR-2.5	an AI query module that enables users to submit queries to DI platforms in accordance with the rules set in the management environment.
FR-3	The browser plug-in described in FR-2.1 must meet the functional requirements specified in FR-3.1–FR-3.8:
FR-3.1	it must have the functions of creating and submitting queries to the server (see FR-2.2);
FR-3.2	it must have a function for collecting data on websites visited by the user;
FR-3.3	it must have a function for storing a list of illegal websites received from the server;
FR-3.4	it must have a function for comparing the data of the visited website with the locally stored list of illegal websites;
FR-3.5	must have a function for sending notifications to the user. The user must be shown a notification about detected legal or illegal content or the inability to determine whether the content is legal or illegal;
FR-3.6	must have a convenient temporary deactivation function;
FR-3.7	must have a function for collecting data for analytical purposes. The list of data collected for analytical purposes shall be proposed by the Service Provider and agreed with the Contracting Authority;
FR-3.8	must have a function for leaving feedback on distribution platforms and directly to the administering authority.
FR-4	The server side, database, and integration interface modules must meet the functional requirements specified in sections FR-4.1–FR-4.5:
FR-4.1	they must have a function for storing data about websites that distribute illegal content;
FR-4.2	it must have a function for receiving and processing queries from a browser plug-in (providing the plug-in with an updated list of illegal websites);
FR-4.3	it must have a function for submitting queries to external information sources (receiving data, submitting reports);
FR-4.4	must have a function for collecting statistical data on user behavior and other aspects of the TSL (analytical module). The list of statistical parameters to be collected shall be agreed with the Contracting Authority during the prototype development phase;
FR-4.5	must have a function for creating backup copies and restoring data from backup copies. The frequency and rules for creating backup copies can be changed in the management environment.

No.	Requirements
FR-5	The management environment must meet the functional requirements specified in points FR-5.1–FR-5.12:
FR-5.1	it must have a function for authorized users (system administrators) to log in to and log out of the system;
FR-5.2	it must have a function for creating authorized user accounts using a graphical user interface (hereinafter referred to as GUI);
FR-5.3	it must have a function for editing, deleting, and filling in records in the database using GUI. This includes manual editing of the list of illegal and legal websites;
FR-5.4	must have a function for changing the structure of data stored in the database using the GUI;
FR-5.5	must have a function for viewing and downloading statistical reports in formats agreed with the contracting authority (XLSX, CSV, JSON, XML) using the GUI;
FR-5.6	must have the ability to work with user list information (blocking users by identification numbers, checking activity) using the GNS function;
FR-5.7	must have the ability to establish integration interfaces with external information sources using the GNS function. This includes partial or complete updating of the list of illegal and legal websites based on external information sources;
FR-5.8	must have manual processing of user reports of illegal content and automatic processing algorithms using the GNS function;
FR-5.9	must have different levels of authorized users (users with access to the management environment). The levels differ in terms of access to different management environment functions. The setting and assignment of these levels to authorized users is determined using the GNS function. At the start of the system, two types of authorized users are set: an administrator (has access to all administrator environment functionality) and moderator (has access to all functionality, but without editing rights);
FR-5.10	the ability to change the frequency of backup creation, rules, and related settings must be ensured. The function of changing the log storage period must be ensured;
FR-5.11	rules for encouraging users to leave feedback must be ensured. (under what conditions the plugin prompts the user to leave feedback);
FR-5.12	the AI integration module settings must be ensured (supported platforms, daily limit of user queries, and other related functions).
FR-6	The AI query module must meet the functional requirements specified in sections FR-6.1–FR-5.6:
FR-6.1	it must have a function for receiving queries from user plug-ins (the source code of the website to be checked is received);
FR-6.2	it must ensure the application of the maximum daily query limit for users;
FR-6.3	it must have a function to check whether the AI response for this website is stored in the database;
FR-6.4	it must have a function to generate the AI query text according to the rules set in the management environment;
FR-6.5	must have a function for submitting a query to the DI and receiving a response, including all functions necessary for working with AI platforms. The list of supported DI platforms is agreed with the Contracting Authority;

No.	Requirements
FR-6.6	must have the function of interpreting the AI response, forming a record in the database, and submitting the response to the user's plugin.
	Non–functional requirements
NR-1	TSL must meet the following architectural requirements:
NR-1.1	it must implement the principle of scalability. The program code must not limit the performance of the TSL (the number of users connected at the same time).
NR-1.2	the principle of open source must be implemented. The scope and methods of implementing the open-source principle shall be agreed with the contracting authority before starting to develop the prototype;
NR-1.3	it must be developed based on the principle of a modular information system. If necessary, it must be possible to install additional modules or functionalities without reprogramming the TSL.
NR-2	TSL must comply with security requirements:
NR-2.1	the service provider performs a Data Protection Impact Assessment (DPIA, hereinafter referred to as DAPV). DPAV is coordinated with the contracting authority. It must be ensured that the technological solutions applied ensure system protection, management of identified risks, and compliance with good practices;
NR-2.2	in all cases, except where it is impossible to achieve the purpose of the TSL, it is necessary to ensure the anonymity of user data and the automatic deletion of unnecessary data without the possibility of recovery;
NR-2.3	security must be ensured at the browser plugin level and at the database level;
NR-2.4	the connection between the server side and the browser plugin must be encrypted using SSL (Secure Socket Layer) or other equivalent encryption measures.
NR-3	The TSL must meet the speed requirement – at the same time, the TSL should be able to serve at least 10,000 users. The supplier will have to provide speed test results. There should be opportunities to expand the plugin's performance in the future.
NR-4	TSL must meet compatibility requirements:
NR-4.1	it must be ensured that it works in Chrome (as well as browsers that use the Chrome browser engine and support plugins of this type) and Firefox browser versions on Windows, MacOS and Linux platforms, as well as Safari browser versions on MacOS, iOS, iPadOS platforms and Firefox for Android browser versions on Android platforms;
NR-4.2	proper fulfilment of functional requirements must be ensured on iOS, iPadOS and Android platforms, considering the limitations of these platforms.
NR-5	TSL must meet the requirements for convenience and user experience:
NR-5.1	compliance with the user experience requirements set out in the Web Content Accessibility Guidelines (WCAG) must be ensured. These guidelines include, but are not limited to, the following requirements;
NR-5.2	the service provider must submit to the contracting authority three TSL design options, graphically illustrating different TSL scenarios and detailing compliance with the WCAG. Considering the specifics of mobile platforms, a separate proposal must be prepared for these platforms.
NR-6	The service provider must meet the following requirements for the creation and preparation of the TSL for practical use:

No.	Requirements
NR-6.1	the methods of implementing the open-source principle must be agreed with the contracting authority. The Elastic License v2 license must be used, and the source code (after the creation of the TSL) must be published in public code repositories. The service provider is responsible for selecting the appropriate settings for the public code repository in accordance with the procedure agreed with the contracting authority;
NR-6.2	prepare a prototype of the TSL in accordance with the procedure agreed with the Contracting Authority, which would allow for the verification of all functional requirements and non-functional requirements agreed with the Contracting Authority. Verification (testing) must be carried out with people (testers) and with automated testing solutions, which the Service Provider must prepare together with the testing environment. In all cases, functional and non-functional requirements must be properly fulfilled during testing. The accuracy of DI responses must exceed 95%. The following scenarios are tested:
NR-6.2.1	updating the list of illegal and legal sources;
NR-6.2.2	identifying errors in the list of illegal and legal sources;
NR-6.2.3	the occurrence of high load (10,000 people using the technological solution at the same time);
NR-6.2.4	changing settings while the system is running;
NR-6.2.5	loss of functionality of each external system element;
NR-6.2.6	evaluation of different websites;
NR-6.2.7	operation on different platforms (browsers, operating systems);
NR-6.2.8	other scenarios agreed with the Contracting Authority.
NR-6.3	prepare and agree with the Contracting Authority a service level agreement (SLA);
NR-6.4	prepare and agree with the Contracting Authority on the implementation of the responsible disclosure process;
NR-6.5	prepare and agree with the Contracting Authority on the technical documentation and user manual. The technical documentation and user manual must describe in detail the operation of the technological solution, its capabilities and limitations. This must include, but is not limited to, the process of creating and restoring backup copies;
NR-6.6	ensure that the final version of the TSL complies with the requirements of the distribution platforms. The list of distribution platforms shall be agreed with the Contracting Authority;
NR-6.7	the final version of the TSL delivered to the Contracting Authority must comply with all the requirements of the technical specifications and must be fully ready for practical operation.

Source: prepared by Consultant