Protection of minors on the Internet

–

Avoid the inappropriate content by preserving their privacy

February 2020

EXECUTIVE SUMMARY

Access to digital content has become a reality to which all groups of individuals are exposed. Around 85% of the Spanish population has access to the Internet from home and, in particular, almost 70% of children younger than 15 years have a mobile phone[1].

Despite the benefits of today's connectivity, there are a number of risks that we must not forget, particularly regarding the most vulnerable groups such as minors, and we must remember that any event in childhood may have a significant impact on their development as adults. Consequently, while access to the Internet must be considered as a great opportunity for the development of minors, parents or guardians must adopt measures to protect them from the threats of the digital environment, as is done in the physical world, and the industry must provide tools aimed at helping safeguard their privacy and well-being.

This document introduces the main options available to parents and guardians to prevent minors from accessing inappropriate content. Likewise, it includes recommendations for the developers of tools for the protection of minors so that they can apply the technical and organisational measures necessary to protect the rights and freedom of minors.

Keywords: minor, control, parental, privacy, analysis, Internet, device, mobile, GDPR, LOPDGDD, technological unit, content, inappropriate.

[1] INE – España en cifras 2018

TABLE OF CONTENTS

I. INTRODUCTION

Minors' access to inappropriate content is a frequent concern for parents in an increasingly connected world, considering the use of smart devices from very early ages. For example, the age of first access to pornographic content in Spain has fallen to 8 years, and from 14 years onwards the consumption of this type of content is widespread[2].

Examples of inappropriate content for the development of the child are images or videos featuring sexual content, violent content, inappropriate language, fashion that promote negative values that may lead to health risks or bad habits, or false or unsupported information. Access to this type of content does not always derive from an express search of the child, but in many cases there is an "accidental" exposure when this type of content appears unexpectedly when they are carrying out any activity on the Internet.

Consequences for minors are as diverse as they are undesirable, ranging from psychological and emotional damages to the development of dangerous and socially inappropriate behaviours or damages to their physical health.

There are various options to prevent minors from inadvertently or intentionally accessing inappropriate content while they use these devices to browse, use applications, play videogames or watch online TV. These options, which often come in the form of applications for mobile devices, may be very intrusive of the privacy of the child and therefore it is convenient to know the risks so that they may be limited[3].

This document introduces the main options available to parents and guardians to prevent minors from accessing inappropriate content, identifies the main risks posed by their use and outlines recommendations to choose the appropriate tool to minimise the risks to the child's privacy.

Likewise, it includes recommendations so that the developers of tools for the protection of minors can apply the technical and organisational measures necessary to protect the rights and freedom of minors.

II. PURPOSE AND RECIPIENTS

The purpose of this technical note is to underline the harm that may occur to a child when accessing content that is not appropriate for their age, the options available to parents to avoid their children's exposure to this type of content, the privacy implications of these tools, tips for responsible use of said tools and recommendations for developers to comply with the GDPR.

This technical note is mainly intended for parents and guardians of children who wish to promote safe use of technology, who need to establish mechanisms aimed at limiting access to inappropriate content and monitoring children's use of the devices.

It is also intended for entities and developers that make these tools available to parents and guardians through the main mobile device platforms.

Finally, this technical note may be of use for editors and publishers of adult content.

[2] Brage, Lluís & Orte, Carmen & Gordaliza, Rosario. (2019). Nueva pornografía y cambios en las relaciones interpersonales de adolescentes y jóvenes.

[3] Álvaro Feal*, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, and Alessandra Gorla. (2019) Angel or Devil? A Privacy Study of Mobile Parental Control Apps

III. IMPACT OF INAPPROPRIATE CONTENT ON MINORS

Before addressing the possible impact of access to inappropriate content, it is necessary to outline, even briefly, the ways in which minors can access adult content.

Basically, access occurs through direct or intentional search/access, indirect or unintentional access, entertainment and video game content, access through social networks and access through online advertising services.

Direct or intentional search/access takes place when minors access information available on the Internet to satisfy their curiosity, by searching for adult content in search engines and accessing content that is not appropriate for their age, but which is easily available online.

Indirect access occurs when a child unintentionally finds information with inappropriate content while searching or consulting other information.

Entertainment content such as films, television, music and video games may contain a large amount of content that is inappropriate for minors, which is often explicit content: violence, sex, extremist behaviour and values, etc.

Similarly, social networks, including instant messaging services, e-mail, etc. are full of frauds hidden as promotions, discount coupons and online commerce, as well as exchanges of inappropriate content among minors (images, videos, etc.).

Finally, it is worth noting that in the online world advertising is always present in the form of pop-ups, banners, videos, etc. and it may sometimes result in the exposure of minors to inappropriate content such as pornography, gaming and gambling services, etc.

Access to inappropriate content may have numerous consequences for minors, as many as there are varieties of inappropriate content. The Spanish National Cybersecurity Institute (INCIBE) highlights within the framework of its initiative Internet Segura para Niños (is4k.es) the following potential damages to minors:

- Psychological and emotional damages. The maturity and self-esteem of minors are still developing, so they are more vulnerable emotionally if they encounter information that they not capable of assuming or to which they do not know how to react, such as pornographic or violent content. These may be too complex or even disturbing for them.
- Misinformation, tampering and false beliefs. False and incorrect content may confuse minors and is particularly dangerous when it is related to health and safety issues.
- Development of dangerous or socially inappropriate behaviour Minors may assume certain content to be true and positive, and adopt it as harmful behaviour or values: sexism, machismo, homophobia, racism, etc.
- Damage to physical health. Some content is aimed at promoting eating disorders (anorexia and bulimia), self-harm behaviour or drug use. Other contents may encourage minors to carry out activities which are potentially dangerous to their health, such as some viral videos or publications.
- Inclusion in harmful groups and communities. Accessing certain contents may bring the child closer to extremist, violent or racist groups, as well as ideological or religious sects, radical political groups, etc. The emotional factor is important when dealing with this information, which may be harmful or malicious, since low or developing self-esteem increases the vulnerability of the child.

- Addiction. Access to inappropriate content related to drugs, sex and gambling may lead to addiction disorders, since minors may not have sufficient critical capacity to manage the risks associated with this kind of activities.
- Economic costs. Fraud or scam attempts aimed at swindling users to steal their money or data may result in direct financial losses, as is the case with Premium SMS subscriptions. Additionally, children are more vulnerable when it comes to interpreting and managing the excessive advertising they are exposed to on the Internet, as it may generate in them the need to consume impulsively, as is the case with purchases in games and applications. Likewise, the content of the ads is not always suitable for them.

IV. OPTIONS TO AVOID ACCESS TO INAPPROPRIATE CONTENT

Below is a non-exhaustive list of options that may help prevent minors' access to inappropriate content, or at least limit such exposure to the extent possible.

A. SAFE SEARCH ENGINES AND APPS WITH EXCLUSIVE CONTENT FOR CHILDREN

The most immediate and obvious option to prevent minors from accessing content that is inappropriate for their age and maturity level is safe search engines and applications with content exclusively aimed at children.

In general, these are search engines based on Google SafeSearch that exclude search results based on certain filtered words such as Kiddle, applications such as YouTube for Kids, which restrict video searches, or applications with content exclusively aimed at children such as App Movistar Junior and Vodafone Kids Planet, among others. In addition, some of them give you the option to limit browser usage time or block the screen. In general, these are applications that do not violate the privacy of the child, and given their reduced functionality, they do not require a high number of permissions to operate. On the contrary, they are only effective for minors who use the device under direct adult supervision because by changing the application all restrictions are easily avoided.

Some devices (for example, Samsung Kids Home) allow users to set up a PIN-protected environment of permitted applications so that the child can only use those applications. In this way, access to multimedia content and new applications may be authorised as the child's needs increase. This is achieved through a launcher. A launcher is the equivalent of a desktop in Android; it shows the icons of some applications and allows to run them, as well as the wallpaper image, but hides the icons of prohibited applications so that they cannot be run. This mode allows more autonomy for the child with the device, since they can change between the authorised applications and contents, but they are effective only among the smallest ones due to the aesthetics and great restrictions imposed.

B. PARENTAL CONTROL OFFERED BY THE MANUFACTURERS' OPERATING SYSTEMS

The large manufacturers of operating systems for mobile devices offer very comprehensive solutions, either integrated into the system and free or included in the license of the operating system. That is the case of Google's Family Link for Android devices or Apple's Parental Control for iOS devices. In the first case, it is installed as an independent and free application from Google Play Store; in the latter case, it is integrated in the OS and users only have to activate and configure it.

Microsoft also offers the possibility of establishing parental control settings in Windows 10, with some features available in Android via the Microsoft Launcher application, which is also integrated into the operating system itself, but does not include web content filtering.

Both in Google and Microsoft it is necessary to create a specific user account for the minors, indicating their age, and that they will be authorised and managed from an adult user account.

Despite being well integrated into the system, they have limitations. For example, in Family Link, the content filtering feature only works when using Chrome to browse, and it is necessary to block the installation and use of other browsers. In the case of Microsoft, the content blocking feature only works on devices with Windows 10 and the Edge browser, and it requires to block the installation and use of other browsers.

Apart from the content filtering, in general the three options offer similar functionalities, such as application control/blocking, usage time control and GPS location.

The wide range of functions that they offer means that these applications must have access to a large number of protected system resources and must carry out personal data processing of great volume and complexity in relation to the minor, which may be very intrusive for their privacy.

However, in cases where they are integrated into the operating system, they will rarely require any user permissions since they can access the resources through the privileges of the operating system.

For this reason, it is vital that such applications perform an essential transparency exercise in their privacy policies and offer sufficient granularity on the processing to be carried out.

C. OTHER PARENTAL CONTROL APPLICATIONS

There is a wide range of parental control applications on the market which allow users to block access to inappropriate content for minors. The INCIBE is4k website contains a compilation of many of these tools, as well as a selection guide. These applications have very diverse functionalities, such as time control, content filtering, application blocking, activity monitoring, alerts and notifications, multi-device control, geolocation, etc. However, not all of them prevent access to inappropriate content, therefore it is important to choose one that includes content filtering and application blocking features.

As in the previous cases, these are applications that, due to their features, can access sensitive traffic information, the activity of the child on the Internet and even their physical location, so users should choose the application carefully according to the granularity it offers in the features provided and take into consideration their privacy policies before installing them.

Those applications that, among their functionalities, allow the control of the child's activity in social networks will also need to have access to the user accounts of the social networks, and therefore access to the child's information in such social networks. While providing an extraordinary control capacity, which may be appropriate in certain circumstances, they may also involve excessive intrusion into the child's privacy. All social network applications include privacy controls to control/limit the child's interaction with strangers, censor messages received based on their origin and content, etc. The is4k webpage contains guidelines to make the most of these privacy options.

These applications will require from the user numerous permissions to access system resources, which once granted give the applications access to a variety and volume of information that is traditionally reserved for the operating system[4].

Consequently, these applications should also be required to have exemplary transparency regarding the processing of personal data and to apply technical and organisational security measures of the highest standard in order to minimise the risks to the rights and freedoms of minors.

Some of the best-known applications are Qustodio, Norton Family, Kaspersky Safekids, F-Secure Mobile Security and Securekids.

D. OPTIONS OF PARENTAL CONTROL OFFERED BY TELEPHONE OPERATORS

Spanish traditional telephone operators give users the option of contracting a parental control service (Movistar Protege, Vodafone SecureNet and Orange Kids Ready), at an additional cost and which requires the installation of a specific application on each device to be controlled. They allow users to manage children's internet activity, and content filters (adults, violence, social networks, etc.), to define connection periods, to block applications and other features from a single point that controls the managed devices. In the case of Movistar, it is based on another commercial application of parental control named Qustodio.

Only Orange has a specific rate for minors named Orange Kids, which includes the protection of the Orange Kids Ready service free of charge and by default.

E. ALTERNATIVES TO THE USE OF PARENTAL CONTROL APPLICATIONS

There are some alternatives to avoid installing parental control applications, but they require certain technical knowledge. One of them is the DNS content filtering option, offered by OpenDNS (Family Shield), CleanBrowsing and others. It must be configured in the home router[5], changing the DNS servers configured by the internet provider for other DNS servers that will filter the requests for access to websites with inappropriate content (adults, games, bets, torrents, social networks, etc) based on configurable filters. It may be very effective for all devices connected to the home network (WiFi or cable), such as mobile phones, tablets, computers, game consoles and smart TVs, but difficult to manage for mobile data connections and other WiFi networks. Telephone operators used to offer this type of services easily to their ADSL customers, such as Telefónica's CanguroNet.

These alternatives may be used in combination with some of the aforementioned parental control applications.

F. PARENTAL CONTROL IN OTHER DEVICES

Parental control in TV and video streaming services

The main TV and video streaming platforms (HBO, Netflix, VodafoneTV, Movistar+, OrangeTV) offer the option of blocking access to certain content by establishing an access code.

[4] Álvaro Feal*, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, and Alessandra Gorla. (2019). Angel or Devil? A Privacy Study of Mobile Parental Control Apps

[5] Domestic routers setup examples with OpenDNS or CleanBrowsing

Parental control in game devices

All video game consoles have a parental control system that allows parents to protect the safety of their children and maintain an appropriate level of privacy. These applications, among other things, allow users to select which games children can play according to the PEGI rating; limit and monitor online purchases, limit access to Internet browsing from the device, limit game time and control the level of online interaction in game chats.

G. CONTROL METHODS BY CONTENT PUBLISHERS AND EDITORS

So far, there is no evidence that editors and publishers of adult content in Spain use any effective method to verify the age of their users, beyond requests to the users themselves to confirm their age.

However, there are solutions on the market that could solve this problem, such as AgeID, AgeChecked, AgePass, and Yoti, among others. These are third-party services that verify the users' identity and/or age by means of a document, such as a passport or driving license. Once the legal age is verified, the personal information is encrypted or destroyed, so that it is only kept and shared with the adult content service whether the user is of legal age or not.

Yoti offers the option of verifying the age without the need to provide any documents by means of facial analysis technologies. In order to avoid false positives, the system will estimate whether the user is over 25 years of age or not, and that is the only data that it shares with the online adult content service. This service can be tested at https://www.provemyage.com/. In addition, Yoti is the only solution certified by the British Board of Firm Classification, based on a certification scheme for age verification systems that includes, among others, data protection requirements.

The transition towards this type of tools would be a major step forward in terms of proactive responsibility on the part of data controllers.

V. MAIN METHODS TO AVOID PARENTAL CONTROL

The control methods presented in this technical note are not infallible and if the minor has a certain interest and curiosity, they may find mechanisms to elude the limits of access to content. Even if they are not interested, and despite taken measures, children will still be able to access this kind of content as a side effect. The main mechanisms to avoid control of access to content are the following:

1. Use of online proxy to access restricted web content. For example, from https://www.hidemyass.com/es-es/proxy users can navigate to other restricted pages. These pages that work as a proxy can be specifically blocked, but users need to be vigilant and block them if their use is detected.
2. Password discovery. Children are often able to discover the password/PIN code to access the management of the parental control.
3. VPNs. Connecting through VPNs (free or paid) may have a similar effect to using proxies, losing all possible control over content filtering.
4. Connection to unprotected networks (WiFi), for example, the WiFi networks of shopping centres or restaurants. If users choose content filtering solutions based on filtering DNS requests from the home network, the child will be able to browse without any filters by connecting to other WiFi networks. Parental control applications can often filter content regardless of the internet access network used.
5. Portable browsers. Some parental control tools only filter content in certain web browsers. Users must block the installation of other browsers to prevent access to

inappropriate content. However, some platforms allow the use of portable browsers that do not require installation and can be used to avoid the filtering of content.

6. Viewing content through non-blocked services such as Google Images, Google Translate, Wikipedia, WhatsApp, Telegram, etc.

Once these mechanisms have been exposed, it is evident that the different parental control options are not infallible and the only way to tackle this type of vulnerability is to complement the use of these tools with appropriate education on the safe use of technology, the dangers of the Internet and the importance of children themselves being able to adopt their own measures.

It is also interesting and necessary to properly configure the privacy and security options of those applications that allow it. Making good use of these functions is essential to achieve more effective parental control. In INCIBE's IS4K initiative, guidelines may be found for configuring applications such as Instagram, TikTok, YouTube, Whatsapp, etc.

VI. RECOMMENDATIONS FOR PARENTS AND GUARDIANS

Based on the previous considerations, various recommendations are established for parents and guardians:

1. Educate minors about the risks to their privacy and safety regarding the use of mobile technologies. Encourage responsible use of technology.
2. Limit the usage time of connected devices.
3. Let them know that it is necessary to adopt measures for their own safety. Tell them that you adopt these measures for their own good.
4. Use operating systems, Internet providers and third parties that provide parental control options to monitor the use of mobile devices.
5. Configure parental control options, since they offer different features such as content filtering, time limitation, application blocking, social network usage details, GPS location, etc.
6. Choose the tool that best suits your needs and offers guarantees so as not to introduce new risks.
7. Find out about data retention periods and make sure that the data are not used for purposes other than those you need[6].
8. Use browsers, launchers and applications in their children version, which are alternatives that may be less intrusive.
9. Do not forget that other connected devices such as Smart TVs or game consoles are exposed to similar risks.
10. Keep in mind that some tools block excessively, keep open the possibility of unblocking content at the child's request and be open to agree with them the filters and restrictions to be configured. Excessive blocking may be counterproductive.
11. Remember that parental control tools are not infallible, so you must properly configure privacy and security options in applications and social networks[7], stay alert and in communication with your children.

VII. INDUSTRY RECOMMENDATIONS

Since this type of parental control services are mainly offered via applications on mobile devices, it is necessary that the industry, service providers and developers take into

[6] AEPD - Decálogo para la adaptación al RGPD de las políticas de privacidad en internet.
[7] is4k -Configuraciones de seguridad, privacidad y control parental en las aplicaciones de moda.

consideration the recommendations established in the technical note on duty to inform and other proactive liability measures in mobile apps[8] published by this Agency.

Additionally, due to the intrusive nature of this type of applications, motivated by the great functionality that they offer and the special characteristics of the target audience, technical and organisational measures must be applied according to the level of risk to the rights and freedoms of minors.

In addition to the guidelines set out in the above technical note, without being exhaustive, providers of parental control applications should consider the following recommendations:

1. Application of the data minimisation principle. Although these applications often offer a wide range of features, it will not always be necessary for parents to use all of them. Granularity must be offered in this regard, establishing mechanisms that allow each of these features to be activated and deactivated based on the needs of each family. Personal data corresponding to a deactivated feature should not be processed.
2. Minimisation of permissions. Analogously, mechanisms must be established to avoid requesting permissions to access system resources which are unnecessary for the features to be used. As an example, if a user does not need to use the child's GPS location feature, it seems unnecessary that the application has access to geolocation data continuously and even in the background.
3. Management of third-party libraries. Virtually all applications include third-party libraries to add different features, such as usage statistics, error reporting, user authentication, or advertising. In such cases, data subjects must be informed of the processing of personal data that may include such libraries so that valid consent may be obtained before such processing is carried out. Personal data transfers, including international data transfers, for which there is no legitimising basis and without proper information, should be avoided.
4. Establish guarantees for cloud services. It is closely related to the previous section; all mobile applications require a similar set of features offered through backends. In some cases, backends offered by third parties will be used for each of the features, while in some cases these backends will be tailored for the specific application and consumed from the application by means of an API. Regardless of the modality, these backends are usually hosted on servers in the cloud. In such case, the processing carried out by these cloud service providers should be regulated by a contract or legal bond which fulfils the requirements established in the GDPR. The data controller must show diligence in the selection of the cloud service providers, and the contract for commissioning the processing must fulfil the requirements set out in the GDPR, paying special attention to privacy measures from the design, by default, of security, confidentiality agreement and procedure for managing security breaches. For additional information, you may consult the guide on contracting cloud services[9] published by the Agency. Although this type of service is usually contracted by adhering to contractual clauses established by the cloud service providers, the latter should either adapt these clauses to the requirements of the GDPR or provide sufficient flexibility to the contracting systems so that the contracts established may fulfil the requirements of the GDPR.
5. Apply security measures. Considering the volume, categories and profile of the data subjects whose data are processed, the measures must be maximised by applying the highest safety standards.

[8] AEPD – The duty to inform and other accountability measures for mobile devices.
[9] AEPD – Guía para clientes que contraten servicios de Cloud Computing and Orientaciones para prestadores de servicios de Cloud Computing.

VIII. CONCLUSIONS

The use of connected mobile technologies by minors is increasingly spreading and is an unstoppable trend due to the countless advantages that it offers for their development and training. However, it also poses some risks that must be addressed.

One of the most significant risks is the exposure of minors to inappropriate content, such as sexual images, violence, gambling, etc. This exposure may have a significant negative impact on minors, ranging from emotional or psychological damage to the establishment of dangerous and socially inappropriate behaviour or damage to their physical health.

This technical note outlines different options available to parents and guardians aimed at controlling and limiting the exposure of minors to inappropriate content.

The first option is the use of search engines, applications specifically aimed at children and launchers that prevent children from accessing other type of applications. That is a relatively simple and effective option at early ages, but requires vigilance.

Secondly, there are parental control applications provided by operating system developers, telephone operators and other companies. These options, in addition to filtering content, offer additional features such as device usage time control, application access blocking, usage time control by application, activity control in social networks, remote management for parents and guardians, and even real-time GPS location of the minor.

In order to offer all these features, these applications require numerous access permissions to protected resources on the device and to process a very high volume of personal data of the minor. Ultimately, these are effective options in terms of the control purpose they pursue, by they are also very invasive of the child's privacy.

Before choosing a parental control application it is important to obtain accurate information about the personal data processing that will be carried out by the application, in particular security measures, data retention times, possible data transfers, a clear identification of the data controller and how to exercise the rights conferred by the GDPR. It is also important to choose the option that best suits the functionality required, taking into consideration that the greater the functionality, the greater the potential invasion of the privacy of the minor, and the greater the risk that a security incident may affect their rights and freedoms. Special attention must be paid to the privacy settings of each application or social network used by the minor.

Those who make these applications available to parents and guardians must be exemplary in the exercise of transparency and active responsibility, offering sufficient granularity in the features offered and therefore in the processing of personal data. In other words, even though an application can provide precise location of the child, if their parents do not consider it necessary to use it, they should be able to waive the processing and deny access permissions associated with said processing, without this preventing them from using the application.

As an alternative to parental control applications, there are other tools that prevent access to inappropriate content through the configuration of DNS servers that will filter and not resolve those requests that may direct the minor to this type of content. These options are quite effective solutions in home WiFi networks, but they lose their effectiveness when the device is connected to a different network or uses mobile phone connectivity.

In addition to the actions that are the responsibility of parents, some options have also been presented for publishers and editors in order to prevent minors' access to inappropriate content. At present, this type of controls is not very popular, but it is expected that their implementation will be greater in the future. Said measures may be seen as examples of active responsibility in the application of the data minimisation principle.

This technical note also outlines some of the main techniques through which the minor could circumvent parental control, some of which require some technical knowledge, but many others are practically within the reach of anyone with a sufficient level of curiosity and motivation.

Finally, and as a compilation of the information discussed in the technical note, a list of tips is provided in order to avoid the damage that may be caused by the child accessing inappropriate content, but at the same time with the utmost respect for their privacy and intimacy.

IX. REFERENCES

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relating to the protection of natural persons in relation to the processing of personal data and the free circulation of these data and repealing Directive 95/46/EC (GDPR).

Organic Act 3/2018, of 5 December, on Protection of personal data and guarantee of digital rights

https://www.is4k.es/necesitas-saber/contenido-inapropiado

https://www.is4k.es/de-utilidad/herramientas

Brage, Lluís & Orte, Carmen & Gordaliza, Rosario. (2019) Nueva pornografía y cambios en las relaciones interpersonales de adolescentes y jóvenes.

Álvaro Feal*, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, and Alessandra Gorla(2019). Angel or Devil? A Privacy Study of Mobile Parental Control Apps

AEPD - Decálogo para la adaptación al RGPD de las políticas de privacidad en internet.

AEPD – Nota técnica: El deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles.

AEPD – Guía para clientes que contraten servicios de Cloud Computing.

AEPD – Orientaciones para prestadores de servicios de Cloud Computing.

Mobile Security Framework - MobSF

Control Parental iOS – Política de privacidad

Control Familiar Microsoft – Política de privacidad

Family Link – Política de privacidad

Movistar Protege – Política de privacidad

Vodafone Securenet – Política de privacidad

Orange Kids Ready – Política de privacidad

Kaspersky Safekids – Política de privacidad

Securekids – Política de privacidad

Qustodio – Política de privacidad

F-Secure Mobile Security – Política de privacidad

Norton Family – Política de privacidad

X. APPENDICES

Comparative table of the parental control tools analysed

PARENTAL CONTROL TOOLS	CVSS - MobSF	Score - MobSF security	Numb of permis/esons requeste	Trackers - MobSF	Content filtering	Time control	App blocking	Activity in socia networks	Call control / SMS	GPS location	Remote management / Parent A	Operating System	Cost
KASPERSKY SAFEKIDS	6	15/100	27	5	Yes	Yes	Yes	Paid version (Facebook)	No	Paid version	Yes	PC, Mac y Android (iOS only content filtering)	Free and paid version 14,95€/year
FAMILY LINK	6,3	0/100	9	1	Yes	Yes	Yes	No	No	Yes	Yes	Android	Free
SECUREKIDS	6,1	10/100	36	5	Yes	Yes	Yes	No	No	Yes	Yes		Free
QUSTODIO	5	65/100	24	7	Yes	Yes	Yes	Yes (Facebook,	Yes	Yes	Yes	Windows, Mac, Android, iOS, Kindle	After 30 days 42,95€/año (for 5 devices)
CONTROL FAMILIAR MICROSOFT (LAUNCHER)	•	•	•	•	Yes	Yes	Yes	No	•	Yes	Yes	Windows (PC and mobile) Android (with	Included with Windows
CONTROL PARENTAL IOS	•	•	•	•	Yes	•	Yes	No	No	No	No	iOS (iTunes on the PC and Mac)	Included with iOS
F-SECURE MOBILE SECURITY	6,2	10/100	48	2	Yes	Yes	Yes	No	No	No	No	Android	7,45€ / 6 months
NORTON FAMILY	5,7	10/100	10	4	Yes	Yes	Yes	Yes	No	No	Yes		
MOVISTAR PROTEGE	5,5	25/100	22	4	Yes	Yes	Yes	Yes (Facebook,	Yes	Yes	Yes	Windows, Mac, Android, iOS, Kindle	2,99€/month (for 10 devices)
CIBERALARMA	5	65/100	6	1	Yes	No	No	Yes	No	No	Yes	Android	11,90€/year 1 device 56,90€/year 5 devices
VODAFONE SECURENET	6,3	10/100	12	2	Yes	Yes	No	No	No	No*	Yes	Android, iOS	Free in some telephone rates 1€/month for the rest
ORANGE KIDS READY	5,2	55/100	19	4	Yes	Yes	Yes	No	No	Yes	Yes	Android, iOS	2,95€/month(for 10 devices)
SAMSUNG KIDS MODE (Launcher)	6,1	45/100	9	0	Yes	Yes	Yes	No	Yes	No	No	Android	Incluided with Samsung devices

This table includes the values of four parameters obtained through the static analysis of the parental control applications included in the table. The tool used for the analysis is the Mobile Security Framework, an open-source and free tool. Only the Android versions of the applications have been analysed. The meaning of each parameter is detailed below.

Parameter	Meaning
CVSS- MobSF	Rating system developed to provide an open and standard method to estimate the impact derived from vulnerabilities identified in IT. An average of the potential vulnerabilities detected is obtained. Severity is considered low if the rate obtained is between 0.0 and 3.9. Severity is considered average if the result is between 4.0 and 6.9. Severity is considered high when the rate is between 7.0 and 10.0
Score – MobSF	Security score obtained by MobSF on a scale of 0 to 100, depending on the static analysis. Based on the OWASP methodology
Number of permissions requested - MobSF	Number of permissions to access system resources declared in the application code and that would be requested from the user.
Trackers - MobSF	Number of tracker libraries or URLs identified in the application.