

The Dark Side of Social Networks:

Personal Data and Respect for the Privacy

The issues related to the modes and the risks in the use of the Social Networks are very topical so that, in Italian schools (and not only), have been recently proposed and then developed several projects that are dealing with the implementation of specific instructions and use terms for both pupils and parents. Our research investigates the conscious use of social media and the related measures to be taken, or that have been adopted until now, to protect the minors.

Keywords: social network, privacy, minor, data policy, web.

Introduction

The research started following a training course organized at a primary school in Italy and ended with a correct awareness of the use of social networks by parents (media education).

The parent axis, focused on the dimension of learning to defend against the risks of new technologies / social networks and to be closer to the children and the reality that surrounds them, better, intended to provide cognitive tools addressed to adults for power to read, to prevent and, as far as possible, to counteract phenomena such as those concerning cyberbullying.

1 Digital media opens up new forms of understanding, knowledge,
2 expression and criticism, often extending the possibility of access to
3 knowledge by all children or young people. Thanks to the technologies, our
4 students have access to information in a much faster time than in the past, they
5 immediately connect knowledge with images and immediately span possible
6 connections between different fields of knowledge.

7 The knowledge of new media and the conscious use of social media is
8 essential to make parenting responsibility act in a world that is deeply marked,
9 enriched and provoked by new digital tools.

10 Technologies are an indispensable tool for everyday life and we must not
11 forget that children make it a constant consumption, often not mediated by
12 adults who recognize or are called to recognize, essentially, their multiple
13 function and in particular that of entertainment for children.

14 Based on studies already carried out, it is undeniable that the Internet is
15 now widespread and available also on mobile devices. This means that more
16 users are logging in and the values also change according to age (Ceron, A.
17 Curini, L., Iacus, M. 2014) and especially among young people, the
18 phenomenon of use embraces a catchment area that transcends territorial
19 boundaries, but with common and constant factors. But, what lies behind all
20 this? Here is our contribution.

21

22

23

Methodology

Among the research methods, priority was given to statistical surveys on users (survey), content analysis, the experimental method, and case studies.

1) The investigation was fundamental because it is a method commonly used by researchers and marketing scholars who are the real experts, better, communication experts. In our case, a specific population sample was applied to better study: users who use social media.

The survey allowed us to make generalization about the population and therefore a reasonable approximation / probability margin.

The method of collecting information was the interview using anonymous questionnaires administered online with a module for the purpose created.

To obtain a good degree of standardization in the same research, from the initial phase to the final one, the interviewees completed a choice questionnaire, exactly, a set of clearly and explicitly formulated questions in which each question corresponds to a variable provided in the drawing of research.

The data collected allowed both to describe the population examined and to find possible correlations to make comparisons between the different users of social media.

2) In order to carry out an accurate and systematic analysis of the messages on the net, content analysis or 'content analysis' was used, the analysis criteria and a survey form were established (a further questionnaire was articulated in specific problem areas codifying textual elements such as, for example, posts).

The elements were then treated as statistical data and processed by applying the relevant statistical analysis procedures.

3) The experimental method. To establish certain cause-effect relationships the researcher must resort to the controlled environment that is typical of the experimental method. The research drawings related to the experimental method allow the researcher to greatly reduce (sometimes eliminate) the risk that alternative hypotheses threaten the validity of the conclusions of his own investigation. This method substantially implies the complete control of a factor or variable, of which the causal role is supposed, and the control on the selection of the subjects-cases that constitute both the experimental and the control group. It is necessary to select two identical groups: the experimental group and the control group. The members of each group have the same characteristics with respect to all the known variables. The experimental group is subjected to "treatment" and the control group is not. The effect of the treatment on the first group is then monitored and compared with the behavior of the

1 components of the second group. The major advantages of this method lie
2 in the capacity for control and logical rigor that it offers.

3
4 4) To identify / identify common traits of the sample in question (the
5 study was done on a sample of 240 people who were parents of school
6 pupils) on the use of the social media subject of the research and to have a
7 more horizontal horizon, the case study focused on two particular aspects:
8 data and privacy.

11 Findings/Results

12
13 The research, started from a training aimed at parents, which encouraged
14 dialogue and the meeting between the same, so that together they could ask
15 critical questions and without prejudices.

16 What was interesting was, in fact, that it made them estimate the dangers
17 of the network; enthusiastic participation has also put adults in relation to the
18 knowledge of digital participatory practices that entertain our children.

19 The digital tends to reject users because it is complex, new, fast: being
20 able to look out with a small toolbox to its decoding I think it was an important
21 opportunity for the Italian school that was able to grasp the relevance of the
22 problem and respond / return adequate means to parents.

1 It is important to understand that the network does not need only the
2 "banal" place of entertainment, but also skills, "in-depth" information, rights.

3 The request emerging is therefore to follow up on this wonderful
4 experience that has taught so much to all the subjects involved in the school
5 environment and therefore to the stakeholders, and this is why it is fundamental
6 to extend the experience and results at the global level so that everyone can
7 benefit results emerged and continue to unmask all that is hidden behind the
8 well-curated graphical interface on the surface but that could hide behind the
9 scenes aspects unknown to newbies or to the unwary, in short, to all those who
10 surf not informed on the web or who click reading superficially what instead
11 concerns us deeply.

12 For the sake of scientificity, both at the beginning and at the end of the
13 course, initial tests were administered followed by final questionnaires to close
14 the open parenthesis in this great social sea that is difficult to control without a
15 particular knowledge.

16 To check the progress achieved, all the results have been tabulated and, as
17 can be seen from the graphs, the data that emerges between the tests is the
18 marked improvement in the use of social media and the recognition of some
19 fundamental data such as the personal ones themselves: from 39.1% initial to
20 100% final.

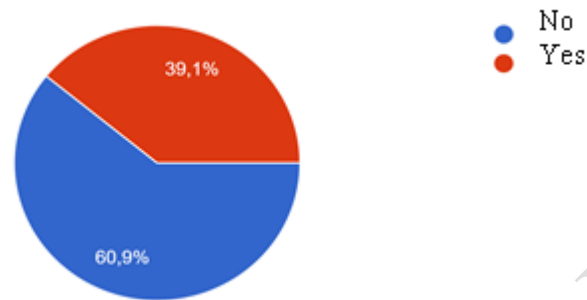
21

22

1 **Figure 1. Item Personal Data.**

2 Question: According to you, those listed are all personal data?

3 *School name - father's name - pet name – pseudonym.*



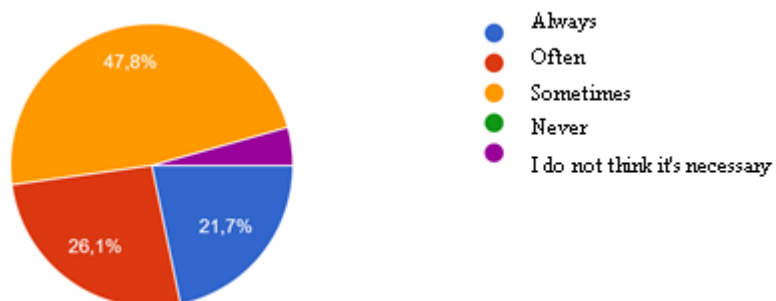
4

5

6 **Figure 2. Item Use Policy – Privacy.**

7 Question: When you publish information about your personal data / your

8 daughter / child on the Internet, are you aware of the privacy or use policy?



9

10

11

12

Discussion

We know that the Web (hypertext and hypermedia that are on the Net) does not coincide with the Internet, as it is a larger and global reality that provides access to services that (we could say "infinite") and content.

The distances have been, in fact, shortened as well for the times to the point that everything is now available and accessible (omnipresent I would add) and if we speak of a precious resource in many fields (I refer in particular to research) ranging from work to communication (which is the sore point), on the other, it puts us in front of great questions that concern young people and adolescents who do not manage (including parents) in depth the spaces that are offered to them.

But what has become "Internet"? We are well beyond the "*World Wide Web*" (as already anticipated): we communicate with email or certified mail (which has superseded the paper or ordinary), we transmit video or speak (voice data) in the network without using the obsolete traditional telephone, if people intervene in the forums and write in the chat rooms (often forgetting the netiquette), the virtual communities, like for example, are depopulated.

Facebook

Of course it is not easy to juggle the various Apps that populate the "Store", but remember that not all of these are the same and coinciding with

1 each other especially in terms of privacy and quality of services or in the
2 processing of our data (which is what we are here we care about it in
3 particular).

4 The not inconsiderable element that is right to bring to the attention is the
5 identification or control of a registered user who has a "friendship" online with
6 us: you can see from a simple "green ball" if, for example, a partner is
7 connected (just tap on the "Activate" tab and select "On" - the button next to
8 your name), or the hours that have passed since the last connection made by the
9 controlled subject.

10 Whoever wants to verify other activities does not stop here; in fact, the
11 "recently added friends" are visible and this, in the case of some bad guy, could
12 mean giving the possibility (without wanting) to peek at the established
13 contacts (unless you select the pencil icon and change the privacy setting to
14 "just me or friends" and among them still discriminate with additional
15 restrictions on the shares that will be later made, finally, there is the option
16 "Personalized" - configurable slightly different but substantially the same for
17 the smartphone - which consists in sharing the images with lists of people or
18 some person) and not for all is a positive factor, which is why to protect
19 yourself and in particular for children, good practice would be to hide the list
20 of friends instead of making it public as expected by default (the entry
21 "Friends" is easily found immediately after "I personal information" and
22 "Photos").

1 Several dangers could also be hidden between the easy clicks on "like": are
2 you sure you have put a "like" on the right picture? And if the photo is public?
3 The whole world will be aware of it and will know trends, habits, customs and
4 much more just to have acted with such haste (typical of young people).

5 In the same way, the "Photos liked by" command is dangerous, followed
6 by the name of the person spied on by someone: unexpectedly and suddenly
7 the photos that the guy has put "Like" will be shown.

8 The ideal solution is to enter an unlock PIN for the various activities on
9 this social network analyzed or insert parental controls among the available
10 Apps (basic applications for attentive parents who want to monitor their
11 children's activities correctly (90% is however pay and therefore represents an
12 increase for less well-off or prepared families).

13 To protect yourself, you need to implement some of the following
14 stratagems, that is, customized security settings:

15

16 1. do not index the profile (visibility);

17 2. disable the face tag;

18 3. control access to data and apps;

19 4. make the photo of your profile not clickable;

20 5. set the OTP (tick "request a security code to access my account from
21 an unknown browser").

22

23

1 **Twitter**

2

3 This "micro-blogging" service allows you to communicate through short
4 messages (tweets) of a few characters, photos and videos, to use it you must
5 register.

6 Here there are no "friends" like on Facebook but follower and following
7 (people who follow our updates since we sign up and people we follow).

8 When a user creates his profile on Twitter the immediate result or default
9 (default) is to be "public" and this indicates that tweets can be seen by
10 everyone without restrictions or exceptions, even without prior authorization
11 from those who created the account (later then those who are more attentive to
12 privacy have the ability to change this setting.

13 To protect your profile you must first set among the choices to protect the
14 viewing of content, that is, check the item "Protect my Tweets" and so future
15 updates will be readable only after the acceptance of a possible request for
16 contact.

17 The security part contains the basic settings for defining a higher and more
18 secure access level for your account, which will be configured by sending a
19 code to the mobile number entered and which will be used to access the profile.

20 Watch for Twitter not to propose sponsored messages that will be adapted
21 to the sites visited recently and remember the choice made on the team
22 function of "*TweetDeck*" because it can be carelessly allowed, to more people,
23 to use the same Twitter account.

1 All information on the management / distribution of personal data can still
2 be configured from the page dedicated to their data on Twitter; very useful is
3 the possibility to verify unauthorized access through the chronology (there is
4 also that of the devices to be controlled).

5 If we believe that someone can make offenses against us you can block
6 this user (who will no longer: follow our updates, send us messages, tag us) or
7 remove him from the voice by hiding the tweets, here there is no reciprocity as
8 on Facebook and it is not said that a subject will return the courtesy to follow
9 us.

10 The burning question is whether members check all these settings.

11

12 **Instagram**

13

14 We are in this social, in front of the maximum case of sharing where
15 privacy crumbles, indeed, it is more urgent to run for cover mainly hiding the
16 geo-referencing (or "geotag" eliminating the place where it was taken) from
17 our photos, also delimiting the use of hashtags and manually approving the
18 images in which we are tagged

19 For personal data you need to switch to the configuration from your
20 Instagram profile and select the third icon above the photos (you can also
21 proceed with blocking a person or hide our stories) and the profile can be
22 changed from public to private (even if it is a contradiction then go to share
23 photos on other social networks like Facebook).

1

2 **YouTube**

3

4 Every day we use this channel to see or upload some videos but without
5 full awareness of where you are going to join, even the children of three years
6 (about 80% even simply because fascinated by the shape or characteristics of
7 the device they have in hand and without the need to know the commands also
8 because the video starts automatically) use it to watch cartoons and music
9 clips, for example: the special episode of Peppa Pig entitled "*Buon Natale,*
10 *Peppa!*", in Italian, has an average of about 28.263.362 million views but also
11 Masha and Bear are not to be neglected: the episode 13 called "*Nascondino*"
12 was seen 25.198.038 and got 51.946 likes and this because the tv as
13 "babysitter" was surpassed by the Tablet and the smartphone that in the
14 meantime have had the upper hand and always accompany the users in their
15 every daily move, no one but pay attention to the disturbances and side effects
16 that I hide behind the apparent media wonder, in particular we talk about sleep
17 and obesity disorders, aggressive behavior and even language delays that are
18 all related phenomena.

19 Recently, in the United States, and precisely in an article in the well-
20 known magazine "*The Atlantic*", what is defined as an "algorithm that captures
21 children" has been indicted, referring precisely to this very particular social, the
22 alarm derives above all from the debut of the new App known as "*YouTube*
23 *Kids*" that allows you to upload many hours of movies, in addition, the

1 platform was bought by Google and the problem that has arisen is related to the
2 video transitions: each video follows without intervention of the minor and as
3 soon as the other ends immediately, or to go to the next one just tap on the right
4 of the screen to choose the clip immediately after.

5 Now considering that children love to see and always watch the movie that
6 most likes their desire is favored by this large container of video streaming that
7 (behind the scenes) blocks them in front of the screen where they
8 simultaneously insert a series of targeted advertising and sometimes deceiving
9 (there are videos that in fact are nothing more than commercials of toys to buy
10 and that represent a real investment for advertisers or for those who know how
11 to compose a tailored program and know what to show to a targeted audience).

12 We speak of a large community of people from all parts of the world
13 attracted by the many and always updated features to engage the international
14 community asking only a certain level of trust that in terms of millions of
15 users, we understand well, we can't accurately establish how much is therefore
16 respected the expectation seen and also considered that this trust must be
17 shared by everyone. The hope is that everyone can follow the guidelines
18 reported by the social network for YouTube to work as intended and remain a
19 really fun and enjoyable place.

20 What you may not like or that may violate the "*Community Guidelines*" in
21 terms of inappropriate content (especially in cases of cyberbullying,
22 pornography, sexually explicit and violent content that incites / pushes hate,
23 threats, self-harm, suicide attempts, the construction of dangerous or other

1 types of weapons that are not particularly suitable for minors and those who
2 might otherwise misinterpret the video), may still be subject to review by the
3 YouTube staff; to avoid misunderstandings is essential to set the privacy by
4 logging into your account and clicking on the profile photo and then from here
5 select the preferred option and best suited to personal needs: to flag yourself as
6 a visitor or as an audience, or manage videos or delete the history.

7 If the user has given consent, YouTube is authorized to interact with other
8 social networks such as Facebook and Twitter (and not only).

9 Each share, when uploading a video, will be made public and will be
10 visible to any friend or follower, but if we want to avoid it? Just enter the
11 "Linked accounts" section and we will be shown a screen in which to decide
12 how and if to connect the various social profiles of which you are a part.

13 We must also remember that a public video is visible to everyone, even
14 those not subscribed to the channel, in other words, means that it can be found
15 with a simple search on the web, however, a private video will be shown only
16 to a small circle of people and will not be shown on search engines and an
17 unlisted video will only be visible to users who know the link (these options
18 are editable under the thumbnail of the selected video within each individual's
19 account).

20 It is not good to neglect the fact that both YouTube and Google use the
21 history of the surveys carried out to show search results relevant to their tastes
22 and personal preferences that should therefore be "suspended" to better
23 guarantee privacy.

1 Delete the channel and its contents when the user wants it seems an easy
2 thing, harmless and without consequences, however, since the videos can be
3 downloaded, downloaded via some online services or apps and then saved on
4 smartphones and PCs from anyone surfing the net, there is no need to be
5 amazed if these movies reappear or resurface on the web at any time and in any
6 place even without our knowledge, so adults must retain the role of reference,
7 whether it is guardians or parents and whether it is educators, to protect them
8 when they surf the net, among other things, the complaint procedure for the
9 violation of privacy allows us to report episodes in which your image appears
10 on video without being expressed consent to publication; good practice is also
11 to block unwanted users and regularly review the comments before publishing
12 them definitively and without giving them the right weight or importance.

14 **Ask.fm ("the Social of Anonymity")**

16 A network service (launched on 16 June 2010 by Mark Terebin) different
17 from the previous ones and characterized by the "question-answer" interaction
18 (the same name is indicative: "Ask for me") with the idea of writing questions
19 (contained in 300 characters) on the profile / bulletin board of other members
20 anonymously or follow them without them knowing, the only thing to do to ask
21 questions and answer is register on the site (even with a Facebook, Twitter or
22 Vk.com account) that, under the conditions of use, establishes immediately
23 that users must have at least 13.

1 When someone answers a question you need to remember that the answer
2 is visible on the bulletin board of your profile and that others can click on
3 "like". Many controversies have arisen over time, such as that on cyberbullying
4 (the site has responded to some accusations by stating that it has a "reporting
5 function"), the "Hannah Smith" case in 2013 (the 14-year-old from
6 Leicestershire) was emblematic. had unsuccessfully asked for the site to be
7 blocked following insults and calls for self-harm and then committed suicide
8 (Hannah's father, Dave, accused the creators of Ask.fm of culpable homicide);
9 finally, accusations were born for the improper use of the platform as a means
10 for the recruitment of young people by ISIS (in the Washington Post it is
11 explained how they were enlisted to fight in Syria alongside the jihādists).

12 In addition to the services already listed, today we also make broad and
13 inconsiderate use of instant messaging that has ties or constraints with previous
14 ones, such as:

15

16 **Facebook Messenger**

17

18 Among the features offered by the official Facebook messaging service
19 (available for Android, iOS and Windows Phone, online or directly from the
20 social network, but also in "stand-alone" mode by typing:
21 <https://www.messenger.com/>).

22 The strategy implemented to engage users is linked to the integration with
23 Facebook, even better: if there is an acquaintance or a friend who is a member

1 of the social network he will immediately be involved, even without realizing
2 it, even on Messenger where there are it even the group chats, moreover, is
3 guaranteed a support to a whole series of pleasant and catchy (not by chance)
4 extensions to send (among friends) of the stickers or the animated GIF.

5 In addition, the service offers the function of call or video call (optionally)
6 via data connection or Wi-Fi.

7 What should alarm us (unfortunately many overlooked) is the privacy side
8 because the messages, although they are encrypted (and theoretically well
9 protected), tendentially or really could be read by managers or those who
10 (maybe for some reason) ne they request and all this while transferring data
11 from their device to that of the company's used servers. There is also control of
12 the activities of "friends" because every message is highlighted in bold or
13 notified on the home of our device (together with the time / be active).

14 There are, however, the positive aspects such as the ability to chat
15 simultaneously with all the contacts that have been established (since it even
16 supports groups); in all this it is clear that it is not open source (with the
17 resulting consequences).

18

19 **WhatsApp**

20

21 This app created to chat is now known around the world and used daily by
22 users who currently are about 1 billion.

1 His fortune comes from the simplicity of use (very intuitive is the
2 operation) and the fact of being available for installation on all platforms in
3 circulation as: Android, iOS, Windows Phone, Symbian and even BlackBerry,
4 in addition, is also facilitated authentication because only a phone number is
5 required and the possibility of reinstalling the application in a new mobile
6 phone without losing the groups to which the user is registered (in fact,
7 supports group chats in addition to the common voice calls and is available for
8 free the sharing of audio, photo or video files There is certainly no shortage of
9 defects, there are some limitations and shortcomings still untreated enough to
10 push the most demanding subjects and more attentive to their data to seek
11 solutions that better protect the data exchanged.

12 A strong limitation is represented by the non-accessibility of some specific
13 devices such as the Tablet (even if in truth it works on iPad with jailbreak) and
14 deficiency and the web part (which we'll see soon after).

15 WhatsApp does not support the sharing of working documents except that
16 some stratagems are used), then there are different uncertainties about privacy,
17 let me explain: in the current state of work there has been no positive change
18 on the encryption used and developed in 2014 with an end-to-end system
19 (E2EE - concept expressed in 1981 by H. Saltzer, David P. Reed and David D.
20 Clark and subsequently modified but which is applied on the various network
21 protocols, in the case of the Internet the couple is adopted TCP / IP for which
22 the first establishes the connection and operates in an "intelligent" way and the
23 second provides for the routing of the communication along the nodes and

1 operates in a "stupid" way) better known as "*TextSecure*" able to exploit two
2 keys, of which a public shared with the interlocutors and a private one inside
3 the smartphone used by those who have an account, it means that at least in
4 theory the messages can be decrypted only by legitimate senders and recipients
5 (service managers in this way can't access the content).

6 The flaw therefore lies in the technology developed but not fully increased
7 and perfected seen and considered that in practice German researchers have
8 raised some problems that we can't neglect or fall into the unknown. The
9 study, started and published in April 2015, highlights that only
10 communications addressed to Android devices or that start from these are
11 effectively encrypted with the end-to-end system already mentioned (for which
12 it appears that the functions and operations required by the App that use them
13 must be carried out and performed completely in the terminal nodes or end
14 points and not in the intermediate nodes), however, in other platforms this
15 encryption is not available.

16 The end-to-end principle has however several limitations including:

17

18 - it is not possible to apply this corollary to the applications that work
19 on different nodes as in the case of distributed processes;

20 - we do not know for sure which functions are implemented in the
21 terminal node;

22 - the node's tasks are not specified in case the requested functions are
23 not to be satisfied or executed.

1

2 For those of you who want to know the way in which the messaging
3 services guarantee or not the privacy of their subscribers, I suggest looking at
4 the reports drawn up by the *Electronic Frontier Foundation*
5 (<https://www.eff.org/deeplinks/2018/03/secure-messaging-more-secure-mess>)
6 in which it is well specified which programs use this encryption and which
7 help to precisely identify the identity of the subjects that exchange messages or
8 which companies can read the communications between individuals.

9 Remember that we are not describing an open source but "closed source"
10 software, it means that the source code remains unknown to us and it will never
11 be possible to study in depth the advantages and limitations that characterize it.

12 Apart from the implementation of the end-to-end this App ensures that the
13 retention of users' messages is not on the servers normally used for
14 conversations as happens with those of Facebook.

15 Many now access for undoubted convenience to the web service to be able
16 to open WhatsApp even from the computer (you stop on the button with the
17 three dots inside the App and select the item "WhatsApp Web" or "Settings"
18 from the iPhone), to that after selecting "Ok" I understood on the phone screen
19 and framed the QR code (barcode two-dimensional barcode shown in the
20 figure) will be automatically created an association or mirroring (via a cookie
21 or token) between notebook / computer and cell phone that will last until it is
22 connected to the network; the damage that can occur is that caused by the
23 failed check on the sign "*Stay connected*" and the next "*Disconnected*" that

1 would lead to anyone taking our place on the chair to sneak in the
2 conversations left open.

3 For nosy people it is useful to pay attention to the reading confirmations
4 that can be removed in order to prevent knowing the exact time at which the
5 message was read and to maintain high levels of privacy; great the trick of
6 sharing important files via links and not directly with anyone in a group
7 especially.

8 The general advice is not to publish images or short captions about your
9 state and avoid making "knowing too much" about contacts.

10 A visible or constantly updated state at any moment can only
11 communicate, albeit indirectly, the movements and (in the long term) the daily
12 routine.

13 On a regular basis it is better to remove the backups (backup of data) of
14 the application and save the chats that interest elsewhere (e-mail or txt in turn,
15 however, to be deleted) for two reasons: first, for privacy itself because
16 avoiding to keep them on the device will be much more difficult for anyone
17 spy on them, the second reason is undoubtedly the memory savings of the
18 device used.

19

20 **Telegram**

21

22 Among the best applications that use cryptography and that have been
23 created specifically to exchange important messages is Telegram.

1 Its strength is represented by secret chats (communication system that
2 protects both parties).

3 Not even the server will track messages and you can also set the chat self-
4 destruction.

5

6 **Viber**

7

8 It is a fairly complete application because it offers the possibility to
9 exchange messages and make calls or video calls, moreover, it is compatible
10 with various systems (from Android, iOS to Windows Phone) both in mobile
11 and desktop (Windows, Mac and Linux).

12 The number of users is lower compared to the previous ones and the
13 privacy is not guaranteed enough because even if the messages are encrypted
14 during their passage on the servers, an E2EE encryption is not guaranteed and
15 we can't explore it (the source code is closed source).

16 The positive side is that of public chats thanks to which the user can
17 follow the news on various topics or the activities of some famous character
18 (about the Telegram channels); inviting and captivating are the stickers and the
19 games with which to challenge others; interesting is the opportunity to share
20 their designs created freehand in addition to the common chat audio messages.

21

22

1 **iMessage**

2

3 In this case we pass to the messaging system devised by Apple Inc. for
4 users of iOS, MacOS and watchOS in order to guarantee the free exchange of
5 messages, photos, videos, documents, stickers and others through the use of the
6 network (3G, 4 / 4.5G or Wi-Fi).

7 As for the functions made available to the user we can see that the
8 previous systems are much more elaborate and complete even if at the level of
9 encryption and therefore protection is used end-to-end encryption for which the
10 company can't read the messages and consequently the corresponding content
11 until, notice well, the users of the service do not make a backup on iCloud
12 because in this way the data or conversations can be stored on the proprietary
13 servers and be read.

14 The heavy limit is that it has been developed only for users called at the
15 beginning.

16

17 **Skype**

18

19 We do not dwell much on this application because it already enjoys world-
20 wide fame and is used enough both for messaging and for making video calls
21 or simple calls.

22 It has now been acquired by Microsoft, which has enhanced the ability to
23 guarantee the privacy of users by keeping messages on their servers (the

1 downside is represented by the fact that the company could access these data
2 even if for a limited time.

3 Even if the service is not always stable, a strong point is the sharing of
4 files of various types together with the compatibility with the main platforms
5 Desktop/mobile and the ability to support group conversations.

6

7 **Snapchat**

8

9 Speaking of Snapchat as an app to chat seems a little centered but at the
10 bottom it is a system of sharing (both for Android and for iOS) based on photos
11 (which represent the various immediate "*Snap*" as the snap of the fingers) and
12 short videos that after being viewed are "self-destructing". On the privacy side
13 we can say that the Snap displayed by the recipients are then deleted from the
14 servers of the service offered and can't (at least theoretically) recover, those
15 that have not been opened remain encrypted (but decipherable by the company
16 on servers for 30 days.

17 Here it is better to pay attention to users who register Snap instead of
18 managers.

19 The favorable side is dictated by the originality of the idea: to share photos
20 and videos in a new and different way.

21

22

1 **Google Hangouts**

2

3 With Hangouts we move to an instant messaging and VoIP software that
4 was developed by Google and that, in addition to using the Google Chrome
5 web browser (via Gmail and Google+ as shown in the figure), is also available
6 for other platforms such as Android and iOS.

7 Group chat is well supported, indeed, it is possible to share more photos
8 with friends, sticker or video at the same time, and in addition to phone calls /
9 video calls, it is also possible to manage SMS/messages and the integration
10 with Google services, however, for privacy issues here too there are limits
11 dictated by the servers.

12 Even if the messages are encrypted, the Mountain View giant is authorized
13 to read the contents circulating in the Hosts (the keys are proprietary and the
14 software is not open source) but the most serious gap is the lack of full
15 compatibility with other systems as, for example, those used by Windows
16 Phone (it is not present in the store even if some resort to alternative ways to
17 download and install it) which makes it less preferred among users' choices.

18 Just remember that there are many other applications to report but
19 deliberately have not been reported because the research has naturally focused
20 on those most used by users worldwide, among the many we could still in
21 addition, for example, to quote:

22

We can not but note that there is undoubtedly a change caused by the massive and unstoppable advent of digital technologies that has now involved everyone, big and small, albeit in different ways, that is: those born in the nineties (the digital natives) have found immersed since childhood in digital technologies; on the other hand, we find adults (digital immigrants), who grew up in a world that in some ways is completely different because it is made up mainly of television and books, so much so that they experienced the change in a personalistic key.

27

1 navigate without specific references or rules enmeshed by misleading
2 advertising, moreover, the parents themselves are in difficulty in comparing
3 new technologies, social networks and facing new problems related to these.

4 This divergence and diversity between generations put us in front of an
5 important issue about the relationship between parents and children and their
6 relationship in function and in view of the available scenario, the better the risk
7 looming around the corner is the intergenerational gap in the which young
8 people are more and more ready and technologically competent but more and
9 more alone, on the contrary, adults remain and are in difficulty in carrying out
10 their natural guiding role.

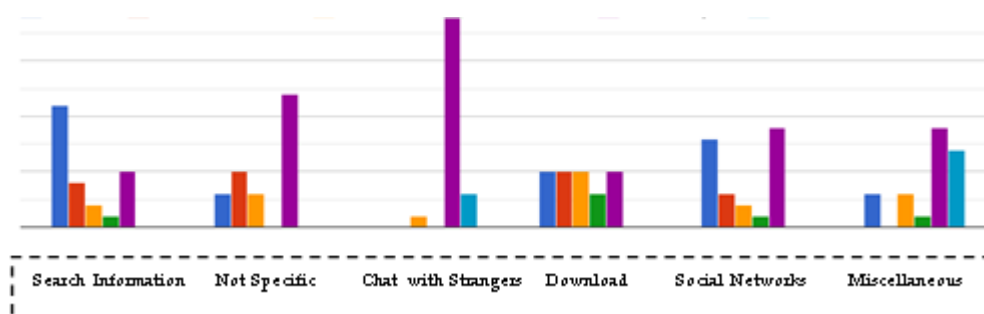
11 The question is not then linked to technical competence or skills: the
12 change we see compromises human relationships and, in our study, that
13 between parents and children, this is why it is necessary for adults to
14 immediately re-think the educational methodology and teaching in all countries
15 and not only in the Italian sample.

16 The hope is to start a reflection on these issues open to all: parents,
17 children and teachers, every problem can be overcome if discussed together
18 and above all with fearless confrontation.

19 Yet, among the various activities carried out in the great global web of
20 communications, it is not really possible to manage the family to precisely
21 manage the online activities of children and young people in general (as can be
22 seen from the graph reported here based on the research done).

23

1 **Figure 3.** *Activities of Children on the Internet (Ratings: 0 - 100%)*



2

3

4

5

References

6

7 Buozzi, B., *Beati e bannati*, Perrone (Luglio 2010).

8 Ceron, A. Curini, L., Iacus, M. *Social Media e Sentiment Analysis* (Gennaio 2014).

9 Donadio, A. *HRevolution. HR nell'epoca della social e digital trasformation*,
 10 FrancoAngeli (Marzo 2017).

11 Emo, T., *Su Myspace sembravi più carino*, Mondadori (Aprile 2009).

12 Norris, S., *Il segretissimo blog di Libby*, Giunti Junior (Luglio 2009).

13 Pax, S., *The Baghdad blog*, Sperling & Kupfer (Settembre 2003).

14 Schwed, A., *Mio figlio mi ha aggiunto su Facebook*, L'ancora del Mediterraneo
 15 (Settembre 2010).

16 Sposini, C., *Il metodo anti-cyberbullismo. Per un uso consapevole di internet e dei social
 17 network*, San Paolo Edizioni (Novembre 2014).

18 Violi, P., *Una mamma da URL*, Dalai Editore (Maggio 2010).