Cyber victimization within the Routine Activity Theory Framework in the Digital Age

Solbey Morillo Puente[1], Iván Neftalí Ríos Hernández[2]
Universidad de Medellín-Colombia

This quantitative-based research determined whether the routine activity theory influences cyber victimization. To measure the dimensions of the theory, defined as *exposure to a motivated offender*, *suitable online target*, and *absence of a capable guardian*, a valid and reliable questionnaire was used. The cyber victimization questionnaire developed by Álvarez-García, Dobarro, and Núñez was applied to 1,285 students selected at random from schools in Colombia. Findings: 46% are identified as *exposed to a motivated offender*, 37.5% are *suitable online targets*, and 29.8% have no *capable guardians*. The interdependence of these three elements revealed that 3.9% of students are at risk due to their routine activities, which had a significant influence on cyber victimization. It is proposed that these findings should be considered in the design of communicative and educational policies aimed at a responsible use of technologies.
Keywords: Cyber victimization, routine activity theory, exposure to motivated offender, suitable target, capable guardian.

Cibervictimización en el marco de la Teoría de Actividades Rutinarias en la era digital
Esta investigación cuantitativa buscaba conocer si la Teoría de Actividades Rutinarias (TAR) influye en la Cibervictimización en una muestra de 1285 estudiantes de secundaria seleccionados aleatoriamente de 11 escuelas rurales y urbanas de Colombia. Se aplicó el cuestionario de Cibervictimización de Álvarez-García, Dobarro y Núñez y se diseñó y validó un cuestionario para actividades rutinarias. Los resultados indican que un 46% está expuesto a un delincuente motivado, 37.5% es un objetivo adecuado en línea y 29.8% no tiene guardián capaz. La interdependencia de las dimensiones reveló que un 3.9% está en riesgo por sus actividades rutinarias, y que hay influencia estadísticamente significativa en la Cibervictimización. Estos hallazgos deben ser considerados por los estudiosos de la conducta por sus implicaciones en la comprensión del fenómeno estudiado y posterior desarrollo de políticas comunicativas y educativas dirigidas a un uso responsable de tecnologías.

[1] Doctora en Educación de la Universidad de Los Andes (ULA-Mérida, Venezuela). Profesora de tiempo completo de la Universidad de Medellin. Dirección postal: Carrera 87 N° 30-65 Medellín – Colombia. Contacto: smorillo@udem.edu.co https://orcid.org/0000-0002-2129-1121

[2] Posdoctoral en Comunicación por la Universidad Austral de Buenos Aires, Argentina. Doctor en Comunicación Social por la Universidad Pompeu Fabra de Barcelona, España. Profesor Auxiliar de la Universidad de Medellín, Colombia. Dirección postal: Carrera 87 N° 30-65 Medellín – Colombia. Contacto: irios@udem.edu.co. https://orcid.org/0000-0002-3926-8480

https://doi.org/10.18800/psico.202201.009

Palabras clave: Cibervictimization, teoría de actividades rutinarias, exposición a un delincuente motivado, objetivo adecuado, guardián capaz.

Ciber-vitimização desde a Teoria das Atividades Rotineiras na era digital
Esta pesquisa quantitativa procurava conhecer se a Teoria de Atividades Rotineiras (TAR) influencia a ciber-vitimização de uma amostra de 1285 estudantes de segunda série, selecionados aleatoriamente entre 11 escolas rurais e urbanas da Colômbia. Foi utilizada a enquete sobre Ciber-vitimização de Álvarez-García, Dobarro e Núñez, tendo sido feito um questionário para atividades rotineiras. Os resultados indicam que 46% fica exposto a um criminoso motivado, 37.5% é um objetivo adequado online e 29.8% não conta com um guardião capaz. A interdependência das dimensões revelou que 3.9% fica em risco pelas suas atividades rotineiras e, que tem influência estatística significativa na ciber-vitimização. Esses achados devem ser considerados por aqueles que estudam a conduta pelas suas implicações na compreensão do fenômeno estudado e posterior desenvolvimento de políticas comunicativas e educativas destinadas ao uso responsável das tecnologias da informação.
Palavras-chave: Ciber-vitimização, teoria de atividades rotineiras, exposto a um criminoso motivado, objetivo adequado, guardião capaz.

Cyber-victimisation dans le cadre de la théorie des activités de routine dans le numérique
Cette recherche quantitative visait à connaître si la Théorie des Activités Rutinaires (TAR) peut influer sur la Cibervictimisation, dans un échantillon de 1 285 étudiants de secondaire choisis au hasard parmi 11 écoles rurales et urbaines de la Colombie. On a appliqué le questionnaire de Cibervictimisation d' Álvarez- García, Dobarro Núñez et on a dessiné et validé un questionnaire pour des activités routinières. Les résultats montrent qu'un 46% est exposé à un délinquant motivé, qu'un 37,5% est un objectif adéquat en ligne, et que 29.8% n'a pas de gardian capable. L'interdépendance des dimensions a révélé qu'un 3.9% est en risque à cause de ses activités routinières et qu'il existe un impact statistiquement significatif sur la Cibervictimisation. Ces trouvailles doivent être considérées par les chercheurs du comportement humain par leurs implications sur la compréhension du phénomène étudié et pour le développement futur de politiques communicatives et éducatives dirigées vers un usage responsable des technologies.
Mots-clés: Victimisation cybernétique, théorie des activités Rutinaires, exposition à un délinquant motivé, objectif adéquat, gardian capable.

Digital convergence has been addressed by countless authors who have provided a reflective look to the issue by analyzing the possible influence of this phenomenon on various sociocultural, technological, media, and academic contexts, among others. According to García (2009), it is "a term that has been used since the mid-eighties to refer to a variety of issues related to the technological transformation introduced by digitalization in the development of telecommunications" (p.104). Jenkins (2008) understands convergence as "culture of media convergence, which supposes the existence of a content flow supported by multiple media platforms, in the cooperation between multiple media industries and in the migratory behavior of media audiences" (p.15). In general, digital convergence is a multidimensional process that affects the cultural practices of society (Bárcenas, 2013).

Studies on digital convergence have traditionally been framed toward understanding this phenomenon from the perspective of communication. However, the social processes derived from the technological unification of this global age have demanded the extension of these studies to new cognitive and thought approaches, configurations leading to collective talks, and generation of new knowledge in the necessary intersection between communication and education.

In fact, from this interdisciplinary integration, one of the aspects that has managed to capture the attention of researchers in both areas of knowledge is related to the influence of routine activities of school children and teens in the risks of using the Internet with emphasis on cyberbullying. Routine activities that frame the behavior of school children and teens with access to various digital platforms or Information and Communication Technologies (ICT) must be addressed by researchers in the social sciences for their potential in identifying risks that may affect the emotional, physical, or academic well-being of this population.

Undoubtedly, the identification of some of the factors and behaviors that may generate risks when using the Internet allows communicators and educators to establish joint prevention strategies for the protection and safety of school children and teens. In addition, it would result in the configuration of thought paradigms and explanatory theoretical models that contribute to the reformulation of management designs and intervention on the appropriate use of ICTs. Amador (2012) points out the coincidences in the cyberculture and hypermediation approaches, indicating that there are three underlying registers that clarify "the relationship between communication, media, and digital technologies versus the subjective and social transformations of the subject: other ways to assume reality; new ways of managing participation; and a rupture of totalization through interactive creation" (p.3).

This new way of assuming the reality proposed by Amador (2012) suggests the need to analyze how the routine activities of children and teens in the network favor their vulnerability to different situations in the virtual space, including cyberbullying. As stated by Miró (2011), "…the risk size generated by the gigantic dimensions of this new social communication space would be different if they had a smaller scope" (page 7).

From the perspective of communication, education, and psychology as interconnected disciplines, it is imperative to analyze whether, in the Colombian context, the access of school children and teens to new independent or collective spaces, characterized by digital convergence, exposes them to some inadequate conducts, including cyberbullying. In this sense, the routine activity theory (RAT) proposed by Cohen and Felson (1979) is applicable to cyberspace and its derivatives due to the relevance it has in understanding the age of digital convergence and the use of the Internet as practices fostering new ways of social interaction between school children and teens.

RAT and Cyber Victimization

The routine activities of children and teens in the network may make them vulnerable to different risks since, as Miró (2011) states, they become risky due to the size and scope of this space used for interaction and communication, in which time and distance are exceeded. Cohen and Felson (1979), authors of the RAT, define this type of activity as "any recurrent and prevalent practice that satisfies the basic needs of the population and individuals, including formal work, leisure, different ways in which people get food and shelter, social interaction, teaching, sexual expression, etc." (p.593). Given its characteristics, cyberspace becomes a stage for cyber victimization. This theory, as applied to cyberspace, emphasizes three interdependent variables: *suitable online target*, described as Internet usage behaviors from a thing or person who is a suitable crime target; *exposure to an online motivated offender,* defined as activities that expose individuals to a cyber-offender when connected to the Internet, and finally, *capable guardian,* which is classified as those people, individual tactics, and technological tools that may prevent potential cyber-crimes (Rodríguez, Oduber, and Mora, 2017).

Some studies on this topic have advanced into the understanding of RAT from different social contexts, resulting in the development of innovative reflections that contribute to further understanding and analysis of this theory starting from a broad perspective. Based on these studies, some of the variables related to the development of risky behaviors that are detrimental to ICT users have already been identified (García-Guilabert, 2016; Álvarez, 2015; Sasson and Mesch, 2014; Llinares, 2012; Pratt, Holtfreter, and Reisig, 2010).

In this sense, in the context of social networks, studies related to RAT have been subject to the identification of some actions performed by Internet users, or intervening variables, which could be classified as risky behaviors for the population who usually uses modern technologies (Shin and Huh, 2011; Sengupta and Chaudhuri, 2011), as well as actions that are subject to the type of communication device and

social network used during the interaction process (Reyns and Henson, 2015; Mitchell, Wolak, and Finkelhor, 2008, Lee and Chae, 2007).

In this research, our analysis focuses on risky behaviors related to cyberbullying, with emphasis on cyber victimization. Cyberbullying has been defined by the Office of the Special Representative of the UN Secretary General on Violence Against Children of the United Nations Organization (2016) as "An aggressive, intentional act carried out by a group or individual using electronic forms of contact, repeatedly and over time, against a victim who cannot easily defend him or herself. This act may include dissemination rumors; posting false or unpleasant messages, embarrassing comments or photos; or excluding someone from online networks or other communications. It is characterized by an imbalance of power and the damage it causes can be profound" (p.14). According to Bauman and Bellmore (2015), the term cyberbullying was popularized by Bill Belsey in 2003, when he launched his www.cyberbullyning.ca website, stating that "although the term had been used in 1993, it is not until 2003 when its use becomes generalized" (p. 1).

Cyberbullying among children and teens has received significant attention from academic researchers in recent years (Kowalski et al, 2014; Cowie et al, 2013; Bauman, Cross, and Walker, 2012; Menesini, Nocentini, and Calussi, 2011; Hinduja and Patchin, 2008). According to Patchin and Hinduja (2006), cyberbullying has been empirically linked to multiple bad emotional, psychological, and adaptive behaviors; hence, its empirical approach is complex.

Just as there are multiple definitions and approaches around cyberbullying, Brown, Demaray and Secord (cited by Kalia and Aleem, 2017a) sustain that there is no standard conceptualization for cyber victimization; however, they suggest that all concepts related to this term contain, among their characteristics, the element of intentional and repeated harm inflicted through the use of technology. The studies on cyber victimization have involved various theories and methodological propositions to explain this phenomenon with a cross-sectional approach. Some have emphasized the development of scales to further

analyze victimization through online social services (Akbulut, Sahin, and Eristi, 2010), while other investigations have framed the object of study to the psychological perspective, consequences, identification of the possible factors of online teen victimization; role of the school in the prevention of this risk; and role of social inequality and networks in cyberbullying(Koutamanis, Vossen, and Valkenburg, 2015; Bauman, Cross, and Walker, 2012; Bauman, 2009; Dilmac, 2009; Dehue, Bolman, and Vollink, 2008; Beran and Li, 2007; Cohen, Kluegel, and Land, 1981).

Cyber victimization is one of the risk behaviors most frequently discussed by recent studies related to the routine activity theory (Arntfield, 2015; Ito, 2013; Livingstone, 2008; Hinduja and Patchin, 2008). According to Marcum (2008), spending a lot of time connected to the Internet, communicating, and sharing personal information online increase the likelihood of being a cyberbullying victim. For the purposes of this research, cyber victims are people who are at the receiving end of cyberbullying behaviors (Kalia and Aleem, 2017b) and who may be related to some of the aforementioned characteristics defined by the routine activity theory (*suitable online target*, *exposure to a motivated offender*, and *capable guardian*).

From the perspective of this study, it is important to determine whether the cyber victimization phenomenon is applicable to Colombian students, considering the guidelines established by the routine activity theory. The findings of this research will serve to establish the explanatory scope of the Theory for the cyber victimization phenomenon in students between 11 and 18 years old and to determine if it is consistent with the studies conducted so far. In addition, they may serve as a foundation for the development of new lines of research using the variables proposed herein. Likewise, these results generate suggestions on prevention matters, which may be used by the government and other public institutions for the design of public policies on these issues.

Purpose of Study

Aligned with the aspects highlighted in the theoretical framework, the variables of this study are as follows: *Routine Activities* are considered as the independent variable of the study. Its dimensions applied to the cyberspace context are a) *suitable online target*, b) *exposure to a motivated offender*, and c) *capable guardian*. The dependent variable was *cyber victimization*, with four dimensions defined by the questionnaire authors (Álvarez-García, Dobarro and Núñez, 2015), namely, a.) visual cyber victimization, b.) online exclusion, c.) identity theft, and d.) written/spoken cyber victimization. As specified above, the purpose was to determine if there is an influence of the routine activities of Colombian school children and teens in cyber victimization.

The study of these variables and dimensions was addressed through a field study and quantitative approach. The research hypothesis was as follows:

> H1. Routine Activities (*suitable online target, exposure to a motivated offender, and capable guardian*) have a statistically significant influence on the cyber victimization of school children and teens in Colombia.

The reasons that justify this study are as follows:

1. From the theoretical point of view, more academic research is required to focus on the study of routine activities and their influence on the risks to which school children and teens are exposed, due to their importance for the identification of intervening process variables. This would allow communicators and educators to establish guidelines to design subsequent prevention strategies aimed at the protection and safety of school children and teens. In addition, the analysis would result in the configuration of new conceptual perspectives and the possible development of explanatory models that contribute to the reformulation of management and intervention

designs on the appropriate use of ICTs for the benefit and protection of school children and teens.

2. From a methodological perspective, it should be mentioned that there is a gap in Latin America of empirical studies, with an emphasis on quantitative methodology developed in the field of communications and education, which may explain the way in which the routine activities of school children and teens have some influence on the risks associated with Internet usage, thus fostering opportunities for the development of cyberbullying behavior and particularly, of cyber victimization. Likewise, the understanding of this process through the information collected in the sample under study with strict measurement scales tends to the adequate interpretation of the data, statistical analysis, and possible replications of this study in other sociocultural contexts.
3. Regarding practical justification, as noted, the results obtained can contribute to the development of prevention and joint intervention strategies among communicators and educators for improving the emotional, physical, and academic performance of school children and teens.

Method

Participants

Data were collected from 1285 female (52%) and male students from grades 6–11, from 15 public schools, both in the urban area (84.9%) and in the rural areas of Antioquia and Chocó (Colombia). 85% of students indicated that their school has an Internet connection and almost half were able to access the network from anywhere (Table 2).

Table 2

Characteristics of the Sample

Variable	Categories	N	%
Gender	Male	617	48.0
	Female	668	52.0
Grade	6th grade	212	16.5
	7th grade	217	16.9
	8th grade	277	21.6
	9th grade	226	17.6
	10th grade	194	15.1
	11th grade	159	12.4
School Location Area	Rural	194	15.1
	Urban	1091	84.9
Internet Connection at School	Yes	1092	85.0
	No	193	15.0
Internet Access Anywhere	Yes	587	45.7
	No	698	54.3

Source: SPSS Results Document

Measures

A three-section self-administered questionnaire was designed. The first section was a questionnaire designed by researchers to measure the three RAT dimensions proposed by Cohen and Felson (1979). This questionnaire was submitted for expert validation and a content validity coefficient greater than .8 was obtained, which is considered optimal. The second section contained the cyber victimization questionnaire by Álvarez-García et al. (2015), which comprises four dimensions. The last section explored aspects such as gender, academic degree, school location area, and Internet connection (Table 1).

We calculated the reliability of the items that constituted the three dimensions of RAT (Table 1) using the *K* coefficient of Richardson

because they are dichotomous variables. In the case of the *Risk Exposure* dimension, the *KR21* value was .57; for the *suitable target* dimension, the value was .71, and for *capable guardian,* the value was .57. Although these results do not reach the optimum value, they can be considered reliable, considering that, according to Nunnally (1967, cited by Frías-Navarro, 2014), "In the first phases of research or exploratory studies, a reliability value of .6 or .5 can be enough" (page 3). In addition, we calculated the dimension reliability for the cyber victimization questionnaire by Álvarez-García et al. (2015) using the Cronbach's Alpha coefficient, as they are additive scales. The results indicated internal consistency of the four dimensions (visual cyber victimization α = .71, online exclusion α = .72, ID theft α = .76, and written/spoken cyber victimization α= .88), as well as for the full instrument (α = .94).

Table 1

Validity and Reliability of the Research Scales

Variable	Dimensions	N_{items}	$\alpha_{Content\ Validity}$	$a_{Reliability}$
Independent: Routine Activities	Exposure to a motivated offender	10	.89	.57
	Target	10	.89	.71
	Capable guardian	7	.85	.57
Dependent: cyber victimization	Visual cyber victimization	5		.71
	Online exclusion	4		.72
	Online ID theft	5		.76
	Written/spoken cyber victimization	12		.88

Source: SPSS Results Document

Routine Activity Questionnaire: This questionnaire was created *ad hoc* by the researchers and comprises 27 items that inquire about the participants' routines on the Internet during the last two months to determine what made them vulnerable in cyberspace. The theoretical definitions expressed by Cohen and Felson (1979) were considered for the design of the items in this questionnaire, which point out three

dimensions: *exposure to a potential motivated offender; suitable online target*, and *capable guardian*, already previously described. For the first dimension, nine items were proposed with an affirmative or negative response. To define as exposed to a motivated offender, the affirmative answer to seven or more items was taken as a criterion.

The second dimension was translated operationally into ten items that represent behaviors that young people acknowledge doing and which expose them to being victimized, considering as such those cases where there are five or more affirmative answers. Regarding the *capable guardian* dimension, it was operationalized from seven items that include the practices or habits that may protect users from cybercrime, as well as activities performed by parents or other family members to control children on teens in cyberspace or which can make them feel controlled (García-Guilabert, 2016). The affirmative response to at least six items reveals the existence of a risk due to the absence of a *capable guardian*.

Cyber Victimization Questionnaire by Álvarez-García et al. (2015): The questionnaire comprises 26 items, measured on a Likert scale of frequency (1 = *never*, 2 = *few times*, 3 = *many times*, 4 = *always*), distributed in four dimensions, namely, visual cyber victimization (five items), online exclusion (four items); ID theft (five items), and written/spoken cyber victimization (12 items). The scores for each dimension were obtained from the sum of the items of each dimension.

Procedure

After the questionnaire was designed, it was hosted on the Google platform and students were asked to answer it online. Stratified and conglomerate random sampling was used. The strata were formed by the six grades that correspond to middle and secondary school in Colombia (6–11). The conglomerates corresponded to a group from each degree at each educational institution to guarantee the representativeness of the sample. The questionnaires were answered anonymously by the students, with prior informed consent, in the computer rooms at each educational institution under the supervision of a teacher, who

did not interact with the respondents. The data were stored in Excel and processed with SPSS 21.

In the descriptive analysis, averages and standard deviation were used for the additive scales, and in the case of the categorical variables, frequencies and percentages were used. The averages of the cyber victimization dimensions were compared according to the exposure, objective, and guardian groups using the Unifactorial Variance Analysis of Fixed Effects at a significance level of 5%. The null hypothesis for equal cyber victimization means of the study groups was subjected to contrast.

Results

The three dimensions of the variable routine activities were explored. The first, *exposure to a motivated offender*, was measured from nine items that reflected the activities that the person does and that expose him/her to risks in cyberspace, such as having a computer with an Internet connection, using social networks, downloading games and music, and not having programs that prevent remote Webcam activation. The presence of at least seven of these behaviors was considered as *exposure to a motivated offender* and allowed to classify 46% of the participants as exposed.

The second dimension, *suitable online target*, refers to 10 behaviors that make children and teens a target for victimization, such as having had contact or initiating friendships with strangers through the Internet, publishing photos or videos or storing personal information on their mobile phones or tablets. Showing five or more of these behaviors represented that children or teen constitute a *suitable online target*. With this criterion, it was found that 37.5% of participants are considered suitable targets in cyberspace.

The third dimension, *capable guardian,* was measured from seven items that refer to the performance of activities that may prevent or foster crimes, such as adult supervision and connection from public

computers or from mobile phones. The performance of at least six of these practices constitutes the existence of risk due to the absence of a *capable guardian* and in the sample, 29.8% of the participants did not have a *capable guardian* who may protect them.

Regarding cyber victimization that constitutes the dependent variable of the study, Álvarez-García et al. (2015) indicate four dimensions: *visual cyber victimization* (five items), *online exclusion* (four items), *ID theft* (five items), and *written/spoken cyber victimization* (12 items). These variables were rated based on the sum of the answers given by teens to the items on a Likert scale of frequency ranging between 1 ("*never*") and 4 ("*always*"). In this sense, *visual cyber victimization*, and *ID theft* had a theoretical fluctuation between 5 and 20 points with a theoretical average of 12.5 points. *Online exclusion* fluctuates between 4 and 16 points, with an average of 10 points. *Written/spoken cyber victimization* comprised 12 items ranging between 12 and 48 points with a theoretical average of 30 points. A higher score on the scales indicates greater cyber victimization.

Empirically, in the students from grades 6 to 11, all averages of the cyber victimization dimensions are below the indicated theoretical average, even in the lower quarter of the scale, while reflecting little variability. In this order of ideas, the average *visual cyber victimization* was 6.4 ± 1.99 points. Similar results were recorded in the *ID theft* dimension, with a mean of 6.23 ± 2.03 points. In the *online exclusion* dimension, the average was very close to the minimum score of the scale, namely 5.1 ± 1.81 points. On the other hand, the average *written/spoken cyber victimization* was 15.6 ± 4.89 points; this value being almost half of the theoretical average of 30 points. These averages reveal that cyber victimization tends to be located at the lower end that corresponds to a low frequency of this risk, while reflecting the "*never*" response in the alternatives.

Considering that the dependent variable is formed by four dimensions in additive scales, which makes it a quantitative variable, and that the independent variable is constituted by the three dimensions of the routine activity theory measured in a dichotomous way (presence or

absence), the Unifactorial Variance Analysis of Fixed Effects was used at a significance level of 5%. Consequently, the following null hypothesis of equal cyber victimization means was subjected to contrast:

> H_0: *Exposure to a motivated offender*, being a suitable target, and not having a *capable guardian* does not influence in a statistically significant way the averages of the four cyber victimization dimensions.

Exposure to a Motivated Offender and Cyber Victimization

It is observed in Table 3 that the averages of the *online exclusion* and *written/spoken cyber victimization* scales for those subjects who were classified as exposed to a motivated offender are higher than the averages for those not exposed, and these differences are statistically significant ($p < .01$). In the *visual cyber victimization* and *ID theft* dimensions, there was no influence of the *exposure to a motivated offender* variable, since the probability values associated with the *F* statistic do not support rejecting the null hypothesis. It is, therefore, concluded that the aforementioned exposure affects *online exclusion* ($F = 13.08$, p = .000) and *written/spoken cyber victimization* ($F = 7.405$; $p = .007$) but not *visual cyber victimization* ($p = .097$) or *ID theft* ($p = .636$).

Table 3

Comparison of Cyber Victimization Means Based on Exposure to a Motivated Offender

Cyber Victimization Dimension	Exposure to a Motivated Offender	**n**	*M*	*SD*	*Min*	*Max*	*F*	*p*
Visual cyber victimization	Yes	595	6.48	1.97	5	19	2.766	.097
	No	690	6.29	2.02	5	20		
	Total	1285	6.38	1.99	5	20		
Online exclusion	Yes	595	5.26	1.90	4	15	13.08	.000**
	No	690	4.90	1.70	4	16		
	Total	1285	5.07	1.81	4	16		

Cyber Victimization Dimension	Exposure to a Motivated Offender	**n**	*M*	*SD*	*Min*	*Max*	*F*	*p*
ID theft	Yes	595	6.27	2.02	5	16	.225	.636
	No	690	6.21	2.05	5	20		
	Total	1285	6.24	2.03	5	20		
Written/ spoken cyber victimization	Yes	595	15.99	4.97	12	43	7.405	.007**
	No	690	15.24	4.80	12	48		
	Total	1285	15.59	4.89	12	48		

** Significant α = .01

Source: SPSS results document

Suitable Target and Cyber Victimization

The second dimension of the RAT refers to the activities that make subjects attractive targets for offenders. The results in Table 4 show that all cyber victimization averages present statistically significant differences. That is, suitable targets report a higher cyber victimization score. We reject the null hypotheses of equal means of *visual cyber victimization* (F = 60.07, p = .00), *ID theft* (F = 16.03, p = .00), *online exclusion* (F = 39.99, p = .00), and *written/spoken cyber victimization* (F = 71.86, p = .00). Therefore, we conclude that the *suitable online target* dimension has a statistically significant influence on the cyber victimization of high school students in Colombia.

Table 4

Comparison of Cyber Victimization Means Based on Suitable Online Target

Dimensions	Suitable Target	n	*M*	*SD*	*Min*	*Max*	*F*	*p*
Visual cyber victimization	Yes	482	6.96	2.19	5.00	19.00	60.07	.000**
	No	803	6.03	1.79	5.00	20.00		
	Total	1285	6.38	2.00	5.00	20.00		
Online exclusion	Yes	482	5.33	1.98	4.00	15.00	16.03	.000**
	No	803	4.91	1.67	4.00	16.00		
	Total	1285	5.07	1.81	4.00	16.00		
ID theft	Yes	482	6.69	2.23	5.00	17.00	39.99	.000**
	No	803	5.96	1.86	5.00	20.00		
	Total	1285	6.24	2.03	5.00	20.00		
Spoken cyber victimization	Yes	482	17.04	5.48	12.00	45.00	71.85	.000**
	No	803	14.71	4.27	12.00	48.00		
	Total	1285	15.59	4.89	12.00	48.00		

** Significant α = .01

Source: SPSS results document

Capable Guardian and Cyber Victimization

When comparing the cyber victimization averages for the subjects included in the *absence of capable guardian* category, it is observed that they are similar to those of the teens considered to have a *capable guardian* (Table 5) and that there are only statistically significant differences in the *visual cyber victimization* averages (F = 5.89, p = .02), but in the other cyber victimization dimensions, the *capable guardian* dimension did not exert a statistically significant influence. We accept the null hypotheses of equal means for *online exclusion* (F = .221, p = .638), *ID theft* (F = .03, p = .87), and *written/spoken cyber victimization* (F = 1.66, p = .20). Therefore, we conclude that the *capable guardian*

dimension has a statistically significant influence on the visual cyber victimization of high school students in Colombia.

Table 5

Cyber Victimization Means Based on Capable Guardian

Dimensions	Capable Guardian	n	*M*	*SD*	*Min*	*Max*	*F*	*p*
Visual cyber victimization	Yes	796	6.45	1.91	5.00	18.00	5.89	.015*
	No	338	6.14	2.09	5.00	20.00		
	Total	1134	6.35	1.97	5.00	20.00		
Online exclusion	Yes	796	5.05	1.73	4.00	14.00	.22	.638
	No	338	5.10	1.92	4.00	16.00		
	Total	1134	5.07	1.79	4.00	16.00		
ID theft	Yes	796	6.22	2.01	5.00	17.00	.03	.872
	No	338	6.20	2.04	5.00	20.00		
	Total	1134	6.22	2.02	5.00	20.00		
Spoken cyber victimization	Yes	796	15.66	4.64	12.00	45.00	1.66	.198
	No	338	15.25	5.17	12.00	48.00		
	Total	1134	15.54	4.80	12.00	48.00		

** Significant α = .05

Source: SPSS results document

Cyber Victimization According to Routine Activities

The RAT establishes that for an aggression to occur, in this case cyber victimization, it is necessary that the three mentioned elements or dimensions are present. That is, it is considered that said contingencies are interdependent. Consequently, it was defined that routine activities become a risk when there is *exposure to a motivated offender*, the subject is a suitable target, and there is also absence of a *capable guardian*. With these characteristics, it turned out that 3.9% of the students who made up the sample are at risk of cyber victimization. When comparing the

cyber victimization averages according to the RAT, it is observed that those who were classified as at risk obtained higher average scores in the four dimensions, compared to those who are not at risk.

These differences in the averages are statistically significant (Table 6), since the probability values associated with the F statistic are lower than the level of significance. Consequently, the null hypotheses of equal means is rejected and we conclude that routine activities influence significantly in visual cyber victimization (F = 9.44; p = .002), *online exclusion* (F = 10.57; p = .001) as well as in the *ID theft* (F = 8.06; p = .005) and *spoken cyber victimization* (F = 13.27, p = .000).

Table 6

Cyber Victimization Means Based on Routine Activities

Dimensions	Routine Activity	n	*M*	*SD*	*Min*	*Max*	*F*	*p*
Visual cyber victimization	Yes	43	7.26	8.12	5.00	19.00	9.44	.002**
	No	1091	6.32	6.43	5.00	20.00		
	Total	1134	6.35	6.47	5.00	20.00		
Online Exclusion	Yes	43	5.93	6.76	4.00	14.00	10.57	.001**
	No	1091	5.03	5.13	4.00	16.00		
	Total	1134	5.07	5.17	4.00	16.00		
ID Theft	Yes	43	7.07	7.84	5.00	14.00	8.06	.005**
	No	1091	6.18	6.30	5.00	20.00		
	Total	1134	6.22	6.33	5.00	20.00		
Spoken cyber victimization	Yes	43	18.14	20.35	12.00	43.00	13.27	.000**
	No	1091	15.43	15.71	12.00	48.00		
	Total	1134	15.54	15.82	12.00	48.00		

** Significant α = .01

Source: SPSS results document

Gender and Cyber Victimization

The results in Table 7 show that males have an average score higher than females in the *online exclusion* dimension, but lower in *ID theft*, and *written/spoken cyber victimization,* with statistically significant differences. Therefore, it can be affirmed that gender influences the online exclusion ($F = 14.31$, $p = .00$), and *written/spoken cyber victimization* ($F = 6.54$, $p = .01$) averages but has no influence on *ID theft* or *visual cyber victimization* ($p > .05$).

Table 7

Comparison of Cyber Victimization Means Based on Gender

Dimensions	Gender	n	*M*	*SD*	*Min*	*Max*	*F*	*p*
Visual cyber victimization	Male	617	6.36	2.07	5.00	19.00	.037	.847
	Female	668	6.39	1.93	5.00	20.00		
	Total	1285	6.38	2.00	5.00	20.00		
Online exclusion	Male	617	5.26	1.95	4.00	15.00	14.31	.000**
	Female	668	4.88	1.64	4.00	16.00		
	Total	1285	5.07	1.81	4.00	16.00		
ID theft	Male	617	6.15	2.03	5.00	17.00	2.28	.131
	Female	668	6.32	2.04	5.00	20.00		
	Total	1285	6.24	2.03	5.00	20.00		
Spoken cyber victimization	Male	617	15.22	4.85	12.00	43.00	6.54	.011*
	Female	668	15.92	4.91	12.00	48.00		
	Total	1285	15.59	4.89	12.00	48.00		

* Significant α = .05

** Significant α = .01

Source: SPSS results document

Discussion and conclusions

The research study tested and rejected the null hypothesis which proposed that *routine activities (suitable online target, exposure to a motivated offender, and capable guardian)* do not statistically significantly influence cyber victimization of school children and teens in Colombia. There is enough empirical evidence to assert that when the three RAT elements are present, i.e., when there is interdependence of the dimensions as established by the corresponding author, there is a highly significant influence in the four types of cyber victimization (*visual cyber victimization, online exclusion, ID theft, and written/spoken cyber victimization*). It can be asserted, therefore, that our research data support the RAT as part of the explanation for the cyber victimization of teens in Colombia.

It should be noted that when the dimensions were analyzed independently, it was observed that being a *suitable online target* influenced all the cyber victimization dimensions. On the other hand, the *exposure to a motivated offender* dimension influenced the *online exclusion*, and *written/spoken cyber victimization*. However, *capable guardian* only influenced visual cyber victimization.

These results are aligned with other studies addressing the routine activity theory and cyber victimization (Kalia and Alemm, 2017b; Ljepava, 2015; Vakhitova, Reynald, and Townsley, 2015) through which it is suggested that the RAT dimensions are a good predictor of cyber victimization in teenage school students. The results of this research also support the important supervisory role of parents as *capable guardians* in the use of virtual technologies, as they can prevent or mitigate the cyber victimization process (Kao, Kluaypa, and Lin, 2017).

As an innovative point of this investigation, it is worth mentioning the dissuasive power a *capable guardian* exhibits for preventing teenage students from being visually cyber-victimized through media such as photos or videos that can be published without their consent. This represents an important point in the identification of factors that can become strategies aimed at preventing cyber victimization when it

comes to visual images disseminated through different digital communication tools.

On the other hand, this research successfully provides support for the applicability of the RAT in the study of the cyber victimization phenomenon among male and female school children, regardless of sociocultural factors, since the results are consistent with other studies conducted in different regions of the world and cited in previous sections. However, it should be noted that in the case of the analyzed sample, males are more likely to be cyber-victimized through *online exclusion* and females are victims of *spoken cyber victimization*, which would lead to subsequent studies that may validate the findings of this research and analyze the causes of this trend. Therefore, the prevention of cyber victimization must consider gender differences to establish policies and actions aimed at strengthening teenage aspects that allow them to reduce their likelihood of becoming victims considering the relationship with the variables proposed by the RAT.

In conclusion, the study showed that for school children and teens in Colombia, the possibility of being a *suitable online target*, being exposed to a motivated offender, and the absence of a *capable guardian* facilitates cyber victimization, with psychological, social, and academic consequences derived from said situation. This implies that school authorities and professionals must work jointly to develop initiatives to prevent school students from exposing themselves to cyber victimization. It is suggested that to advance further in the understanding of the RAT, academics put into practice the key theoretical concepts that emanate from the different research studies conducted to date and develop new methodological alternatives that provide more cross-sectional analysis on the possible influence of the cyber victimization theory in different sociocultural contexts. This may provide the opportunity to redefine prevention strategies that different school and government agencies have been implementing thus far for the protection of school students.

For future research, we recommend further exploring digital communication tools that have the greatest influence on cyber victimization,

considering the routine activities theory as a framework for analysis. We also suggest determining the possible influence that family relations and parent mediation may have on cyber victimization, based on their commitment to the emotional, educational, and social well-being of school students. Finally, it is considered important to discuss the integration of other interactivity platforms, such as video games, in the analysis of the RAT, as well as their involvement in risky cyber victimization behaviors in school children and teens. The expansion of these studies can help to strengthen the research carried out so far and broaden the identification of risk factors in different contexts of interaction with technologies, which will serve as support for those in charge of guaranteeing protection and psychosocial development of school students.

References

Álvarez, F. (2015). Un test de la Teoría de las Actividades Rutinarias. ¿Guardianes capaces o eficacia colectiva?. *Revista de Derecho UNED*, (16), 65-80. https://doi.org/10.5944/rduned.16.2015.15247

Álvarez-García, D., Dobarro, A. y Núñez, J. (2015). Validez y confiabilidad del cuestionario de cibervictimización en estudiantes de secundaria. *Aula Abierta*, (43), 32-38. https://doi.org/10.1016/j.aula.2014.11.001

Akbulut,Y., Sahin, Y.L., y Eristi,B. (2010). Development of a scale to investigate cybervictimization among online social utility members. *Contemporary Educational Technology*, *1*(1), 46-59. https://doi.org/10.30935/cedtech/5961

Arntfield, M. (2015). Toward a cybervictimology: Cyberbullying, Routine Activities Theory, and the anti-sociality of social media. *Canadian Journal of Communication*, 40, 371-388. https://doi.org/10.22230/cjc.2015v40n3a2863

Bárcenas, C. (2013). Aproximaciones al estudio de la convergencia digital. *Estudios sobre las culturas contemporáneas*, (19) 38, 9-27.

Recuperado de https://www.redalyc.org/pdf/316/31629858002.pdf

Bauman, S., Cross, D., y Walker, J. (Eds.). (2012). *Principles of cyberbullying research: Definitions, measures, and methodology*. Routledge.

Bauman, S. y Bellmore, A. (2015). New directions in cyberbullying research. *Journal of School Violenc*e, *14*(1), 1-10. https://doi.org/10.1080/15388220.2014.968281

Bauman, S. (2009). Cyberbullying in a rural intermediate school: An exploratory study. *The Journal of Early Adolescence, 30*(6), 803-833. https://doi:10.1177/0272431609350927

Beran, T., y Li, Q. (2007). The relationship between cyberbullying and school bullying. *Journal of Student Wellbeing, 1*(2), 15-33. http://dx.doi.org/10.21913/JSW.v1i2.172

Cohen, L. E., Kluegel, J. R., y Land, K. C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American Sociological Review, 46*(5), 505-524. https://doi.org/10.2307/2094935

Cohen, l. y Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review*, 44, 588-608. http://dx.doi.org/10.2307/2094589

Cowie, H., Bauman, S., Coyne, I., Myers, C., Pörhölä, M. y Almeida, A. (2013). Cyberbullying amongst university students: An emergent cause for concern? In P. K. Smith & G. Steffgen (Eds.), *Cyberbullying through the new media: Findings from an international network* (pp. 165-177). Psychology Press.

Dehue, F., Bolman, C. y Vollink, T. (2008). Cyberbullying: Youngsters' experiences and parental perception. *CyberPsychology and Behavior, 11*(2), 217-223. https://doi.org/10.1089/cpb.2007.0008

Dilmac, B. (2009). Psychological needs as a predictor of cyberbullying: A preliminary report on college students. *Educational Sciences: Theory and Practice, 9*(3), 1307-1325.

Frías-Navarro, D. (2014). Apuntes de SPSS: Análisis de fiabilidad. Recuperado de https://www.uv.es/friasnav/ApuntesSPSS.pdf

García-Guilabert, N. (2016). Actividades cotidianas de los jóvenes en internet y victimización por *malware. Revista de Internet, Derecho y Política, 22,* 48-61. Recuperado de https://www.redalyc.org/articulo.oa?id=78846481005

García, J. (2009). La comunicación ante la convergencia digital: algunas fortalezas y debilidades. *Signo y Pensamiento, 28*(54), 102-113.

Hinduja, S. y Patchin, J. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior, 29* (2), 129-156. https://doi.org/10.1080/01639620701457816

Ito, M. (2013). *Hanging out, messing around, and geeking out: Kids living and learning with new media*. MIT Press.

Jenkins, H. (2008). *Convergence culture: La cultura de la convergencia de los medios de comunicación*. Paidós.

Kalia, D y Aleem, S. (2017a). Cyber victimization among adolescents: Examining the role of Routine Activity Theory. *Journal of Psychosocial Research*, *12*(1), 223-232.

Kalia, D. y Aleem, S. (2017b). Role of Routine Activity Theory in cyber victimization among adolescents: A gendered perspective. *Phonix International Journal for Psychology and Social Sciences, 1*(3), 1-121.

Kao, D, Kluaypa, B. y Lin, H. (2017). The cyberbullying assessment of capable guardianship in Routine Activity Theory. En Wang, G., Chau, M. y Chen, H. (eds.), *Intelligence and Security Informatics.* Springer International Publishing.

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N. y Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin, 140*(4), 1073-1137. https://doi:10.1037/a0035618.

Koutamanis, M., Vossen, H. G. M. y Valkenburg, P. M. (2015). Adolescents' comments in social media: Why do adolescents receive negative feedback and who is most at risk? *Computers in Human Behavior*, *53*, 486-494. https://doi.org/10.1016/j.chb.2015.07.016.

Lee, S. y Chae, Y. (2007). Children´s internet use in a family context: Influence on family relationships and parental mediation. *CyberPsychology & Behavior, 10*(5), 640-644. http://dx.doi.org/10.1089/cpb.2007.9975

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, *10*(3), 393-411. https://doi.org/10.1177/1461444808089415

Ljepava, N. (Noviembre de 2015). Application of Routine Activities Theory to the prediction of cyber victimization. En 49th Annual Convention of the Association for Behavioral and Cognitive Therapies. Paper presentado en la 49th Annual Convention of the Association for Behavioral and Cognitive Therapies IL en Chicago.

Menesini, E., Nocentini, A. y Calussi, P. (2011). The measurement of cyberbullying: dimensional structure and relative item severity and discrimination. *Cyberpsychology, Behavior, and Social Networking, 14*(5), 267-274. https://doi:10.1089/cyber.2010.0002.

Marcum, C. D. (2008). Identifying potential factors of adolescent online victimization for high school seniors. *International Journal of Cyber Criminology*, *2*(2), 346–367.

Miró, F. (2011). La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista Electrónica de Ciencia Penal y Criminología*, *13*(7), 1-55.

Mitchell, K, Wolak, J. y Finkelhor, D. (2008). Are blogs putting youth at risk for online sexual solicitation or harassment?. *Child Abuse & Neglect*, *32*(2), 277-294. https://doi. org/10.1016/j.chiabu.2007.04.015

Naciones Unidas (2016). Tecnologías de la información y de las comunicaciones: maximización del potencial de los niños y protección de los niños contra la violencia en línea, incluida la explotación sexual. Informe anual de la Oficina del Representante Especial del Secretario General sobre la No Violencia Contra los Niños.

Patchin, J. e Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice*, *4* (2), 148-169.https://doi: 10.1177/1541204006286288

Pratt, T., Holtfreter, K. y Reisig, M. (2010). Routine online activity and internet fraud targeting: Extending the generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267-296. http://dx.doi.org/10.1177/0022427810365903

Reyns, B. y Henson, B. (2015). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with Routine Activity Theory. *International Journal of Offender Therapy and Comparative Criminology, 60*(10), 1119-1139. http://dx.doi. org/10.1177/0306624X15572861

Rodríguez, J., Oduber, J. y Mora, E. (2017). Actividades rutinarias y cibervictimización en Venezuela. *URVIO, Revista Latinoamericana de Estudios de Seguridad,* (20), 63-79.

Sasson, H. y Mesch, G. (2014). Parental mediation, peer norms and risky online behavior among adolescents. *Computers in Human Behavior*, *33*, 32-38. http://dx.doi.org/10.1016/j.chb.2013.12.025

Shin, W. y Huh, J. (2011). Parental mediation of teenagers' video game playing: Antecedents and consequences. *New Media & Society*, *13*(6),945-962.http://dx.doi.org/10.1177/1461444810388025

Sengupta, A. y Chaudhuri, A. (2011). Are social networking sites a source of online harassment for teens? Evidence from survey data. *Children and Youth Services Review*, *33*(2), 284-290. http://dx.doi.org/10.1016/j.childyouth.2010.09.011

Vakhitova, Z., Reynald, D. y Townsley, M. (2015). Toward the adaptation of Routine Activity and Lifestyle Exposure Theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice, 32*(2), 169-188. https://doi.org/10.1177%2F1043986215621379

Recibido: 2019-02-26
Revisado: 2021-07-25
Aceptado: 2021-11-17