Is digital crime victimization increasing in Iceland – may the Me-too movement influence how victimization is experienced?

Helgi Gunnlaugsson and Jónas Orri Jónasson,
University of Iceland

Abstract
The first Icelandic study of digital crime victimization was conducted in 2016. According to the results, approximately 13 % of respondents reported digital victimization during the three years prior to the survey. Slander and consumer fraud were the most common types of victimization. Respondents between the ages of 30 to 44 were most likely to have been victimized. In 2018, the survey was repeated using the same questionnaire. As before, the survey was conducted online in cooperation with the Social Sciences Research Institute and solicited information from a sample of circa 2,000 respondents representative of the Icelandic population ages 18 years and older. Approximately 20 % reported a digital victimization in 2018. This suggests a significant increase in victimization since 2016. The increase was most notable in regards to the sexual harassment of women. It is contended that the MeToo Movement of 2017 may have had an impact on the experiences reported by women in 2018.

Abstract
Den første islandske undersøgelse, der fokuserede på kriminel krænkelse over internettet, blev udført i 2016. Ifølge resultaterne rapporterede ca. 13 % af respondenterne, at de inden for de seneste tre år forud for undersøgelsen havde været udsat for krænkelse over internettet. De mest almindelige former for kræneklse var bagtalelse og forbrugerbedrageri. Respondenter i aldersgruppen 30-44 år viste sig at være mest udsatte.

Undersøgelsen blev gentaget i 2018, med anvendelse af det samme skema som i 2016. Undersøgelsen blev også denne gang foretaget over nettet i samarbejde med centret for socialvidenskabelig forskning og udsendt til ca. 2000 deltagere, der afspejlede den islandske befolkning over 18 år. Ser vi en øgning i kriminel forulempelse over nettet? Ser vi andre former for forulempelse end i 2016? Har Me-Too bevægelse i Island haft nogen indflydelse på ofrenes oplevelse af at være krænket?

Key words
Digital crime, cyber crime, victimization, sexual harassment, Me-Too
Cyberkriminalitet, digitale lovovertrædelser, ofre, sexchikane, Me-Too.

Introduction

In recent years, crime control agencies such as the police have detected a shift of criminal activity from the "real world" to the internet. The web has increasingly been used as a source to target victims all over the globe. Through the internet, people worldwide can be connected, giving rise to all kinds of new opportunities including deviant activities and crime. Several internet-related threats are regularly being reported in the mass media, e.g. computer fraud, ID thefts, sexual harassment, cyberbullying and, most recently, cyberwarfare; all of these indicate a new type of threat to public safety in postmodernity.

Today, everyday life involves more and more online time, particularly for those of us living in western societies. Everyday routine tasks are more often taking place online; we pay our bills online, communicate with friends and family, order food, plan holidays, book flights and hotels, etc. According to Eurostat (2019), approximately 98 percent of Icelandic households had internet access in 2017. Icelandic internet access constituted the highest percentage of homes in Europe along with Norway and Denmark. Close by were Luxembourg and Netherlands where 97 percent of households had access to the internet. Icelandic users are also the most likely to use the internet regularly. Approximately 97 percent of internet users in Iceland reported using the internet at least once a week (Sigurðsson, 2015). This figure was the highest percentage of regular internet users in Europe in 2014.

The fact that people spend more time online has opened a vast range of new opportunities for criminal and deviant activities. Such risks have become a part of everyday life and are something about which we are increasingly becoming more aware. Reports of some form of digital crime are becoming a daily occurrence. The social media group at the Reykjavik Metropolitan Police has repeatedly posted warnings on their Facebook page to warn people about online scams and digital crime-related activities. According to a recent local bank newsletter (Landsbankinn, 2019), criminal violations such as buying, selling stolen goods, fraud, id thefts, and illegal downloading are increasingly taking place online. The proportion of digital crime was expected to succeed drug crimes in 2019, with increasingly more sophisticated methods being adopted.

Making sense of digital crime is challenging for criminologists primarily due to lack of a consistent definition. The term *digital crime* has no specific reference

in the legal code yet it is often used in politics, criminal justice, media, and public and academic discussions (Yar, 2013). Digital crime is also almost non-existent in official data. Few offences are reported to the Icelandic police, and studies have shown that a large proportion of offences remain unreported for various reasons. Victims, for example, might be unaware that an offence has been committed and might not consider the incident to be serious, believing that the police would not react; or, they might be embarrassed.

Another challenge of defining cybercrime is that targets can range from governments and multinational corporations to individuals. Therefore, it can be difficult to grasp digital crime as a single phenomenon, it should rather be understood as a range of illegal activities. A typical definition for different forms of digital crimes is that it has been committed using computers or other online platforms (Leukfeldt & Yar, 2016). Instead of considering digital crime a single phenomenon, it should be viewed as an umbrella term used to describe two closely related criminal activities: digital-dependent and digital-enabled crimes. As is apparent from the term, digital-dependent crimes depend on computers, computer networks, or other forms of information communications technology (ICT). Digital-dependent crimes can therefore only exist online and cannot be committed without the use of computer technology. These types of offences include hacking or spreading viruses, which are directed against computers or network resources from other computers. Digital-enabled crimes, on the other hand, are traditional crimes which are amplified in their scale with the aid of computers or computer networks. Unlike digital-dependent crimes, they can be committed without the use of the internet or computers, for example fraud, data theft, and sexual offence (McGuire & Dowling, 2013).

In the criminological literature (Siegel, 2018) different types of digital crime have been identified. First is *cybertheft* which involves the use of cyberspace to defraud people for quick profits such as illegal copyright infringement, identity theft, phishing, and fraud. Second is *cyber deviance* which includes distribution of illegal goods and services such as pornography and drugs. *Cyber vandalism* is the third type, involving the use of cyberspace for revenge, destruction, and to achieve malicious intent. Examples include website defacement, viruses, slander, harassment, image-based sexual abuse, cyberstalking, and cyberbullying. Finally, there is *cyberwar*, involving efforts from enemy forces to disrupt the intersection at which the virtual electronic reality of computers meets the physical world. Logic bombs used to disrupt secure systems or networks are examples of cyberwar.

The focus in this study is on individual victims, examining victimization among the Icelandic public. Our focus is on experiences considered digital-

enabled crimes and deviant activity online that can have an impact on the victim. Not much is known about how widespread digital crime is in Iceland apart from a previous study in 2016. According to the findings of the 2016 study, approximately 13 percent of the respondents reported having been victimized by different types of digital crime in the past three years prior to the survey (Jónasson & Gunnlaugsson, 2016). Slander and consumer fraud were the most common types of victimization. Respondents aged 30-44 years old were most likely to have been victimized.

The objective of this study is to provide new and updated information concerning internet use in Iceland and perceived exposure to digital crime victimization. What is the actual scope and scale of such crimes in Iceland in 2018? What social groups are most likely to be victimized, and what is the most common type of digital victimization in Iceland? Furthermore, we inquired participants about their own illegal and risky behavior online during the last three months prior to the survey. How many admitted to knowingly breaking the law by downloading illegally copyrighted material? How many admitted to visiting pornographic websites online? Does risky behavior of this type have any impact on digital crime victimization? And most importantly, has there been any change in online victimization since the 2016 study mentioned previously, measuring these different types of activities?

Previous Research and Theoretical Framework

According to prior research, identity theft, phishing, sexual offence, and fraud are among some of the most common types of digital crime (e.g. Oksanen & Keipi, 2013; Wolak, Mitchell, & Finkelhor, 2006; Yar, 2013; Ybarra, 2004). Digital victimization tends to be low among the general population but higher among younger online users when compared to older age groups (e.g. Norton, 2016; Wolak et. al, 2006). It has also been reported that children who use social media to a great extent are more likely to be victimized than children who do not use social media as much (Staksrud, Ólafsson, & Livingstone 2013). Residents living in rural areas are also less likely to become victims of digital crime than those living in larger cities (Glaeser & Sacerdote, 1999).

One study showed that more than three million new malicious software such as viruses and Trojans appeared in the first half of 2015 alone (G Data Securitylabs, 2015). Furthermore, data from the US indicate that approximately 10 percent of internet users in 2012 reported being victims of online scams or phishing (Norton, 2012), and in 2014, more than 348 million identities were exposed by hackers (Norton, 2016). Data from a recent National Crime Victimization sur-

vey in the United States showed that about 17 million citizens had been victims of identity theft in 2018 (IIE, 2019). In a survey by Näsi et al., (2015) about 6.5 percent of young people aged between 15 and 30 years living in Finland, the USA, Germany and UK, reported having been victims of cybercrime during the past three years.

Patchin and Hinduja (2016), leading experts on cyberbullying, conducted yearly surveys using large samples of high school youth in the USA. Approximately one-third of high school and middle school students they surveyed reported having been the target of some form of internet harassment. On average, approximately 25 percent of the students reported that they have been victims of cyberbullying at some point in their lifetime. It was also found that girls are just as likely, if not more likely, than boys to experience cyberbullying as a victim or an offender. Other survey results also seem to support these findings. According to the data compiled by the National Center for Education Statistics (2019), approximately 20 percent of the total student body reported being bullied during the school year.

Previous research has shown that gendered communication patterns may make women more likely to experience sexual harassment online than men because of their gender (Herring, 1999; Taylor, 2003). Gender-based violence online has repeatedly been confirmed in different studies. Image based sexual abuse among youth has been examined in Denmark (Harder, Jörgensen, Gårdshus & Demant, 2020) and social media disclosures of sexual violence in Iceland (Sigurvinsdóttir, Ásgeirsdóttir & Arnalds, 2020). In this respect, women have been shown to be disproportionately more affected by online abuse than men (UN Women Broadband Commission, 2015).

In 2017, the MeToo movement began as a global phenomenon sweeping through every aspect of society including Iceland. Women from different walks of life shared their stories of sexual abuse and sexual misconduct they had experienced in their professional life. While sexual abuse is not new, computer technology and social media have become new platforms for this abuse in addition to providing new media to openly reveal these victimization experiences. Nonconsensual exchange of digital sexual images online was, in this respect, recently a leading topic in the local news in Iceland (Bernharðsdóttir, 2019). Politics is no exception to online sexual victimization. More than 40 percent of female MPs in Europe reported, in a recent study conducted by the Parliamentary Assembly (2019), being victims of sexual harassment online during their political tenure in parliament. An interesting question emerges whether any signs of the MeToo movement can possibly be detected in our survey results in 2018, or how gender patterned victimization experiences play out in the findings.

Research in the field of digital crime often employs the routine activity theory (RAT) introduced by Cohen and Felson in 1979. RAT has been used to analyze various forms of criminal behavior including burglary and violence, but has also recently shed light on patterns of online victimization (Leukfeldt & Yar, 2016). This theory has been shown to have a relationship with digital victimization and the likelihood of becoming a victim of deviant behavior online (e.g. Näsi et al., 2015; Marcum, Higgins, & Ricketts, 2010; Pratt, Holtfreter, & Reisig, 2010). Prior social behavior is believed to influence the likelihood of victimization according to RAT. Those who engage in risky behaviors, are poorly guarded, or are exposed to groups of motivated offenders, are more likely to be victimized than others (Holt and Bossler, 2008).

In this study, one element of RAT will be examined, i.e. prior online social behavior and online victimization. Those who report using the internet frequently, according to the theory, are more likely to become victims of deviant or illegal behavior online than users who use the internet less (e.g. Reyns & Henson, 2015; Näsi et al. 2014; 2015). Moreover, according to RAT, we expect those who use the internet for risky activity such as using pornographic material or illegally downloading copyrighted material to be more likely to become victims of digital crime (e.g. Buzzell, Foss, & Middleton, 2006). However, not all scholars agree. Yar (2005) has, for example, argued that digital crime is substantively different from traditional victimization in that virtual environments are spatially and temporally disconnected and relatively unstable unlike physical space. In this study, an empirical opportunity will be provided to analyze the extent to which the concepts of an established theory (RAT) can be used to understand the new reality of online victimization in Iceland.

Data and Methods

The data of this study was derived from a web-based survey with participants older than 18 years old from Iceland. The questionnaire was only available in Icelandic thus only Icelandic-speaking participants could take part in the research. Data collection was administrated by the Social Science Research Institute affiliated with the University of Iceland and the data was collected in May 2018. All participants had agreed to be members of the institutes' panel. We used a stratified sample mirroring for the population in terms of basic socio-demographic variables of age, gender, residence, education level, and income. The sample size was 1800 members of the panel and the response rate was satisfactory or close to 50 percent.

First, we examined how many had knowingly broken the Icelandic law by downloading copyrighted material or visited pornographic websites during the

last three months prior to the survey. The primary purpose was to distinguish between legal and illegal online activity. According to RAT, we would expect those who engage in risky activities online to be more likely to become victims of cybercrime in general.

The second objective of the study was to examine how many of the respondents had been victims of digital crime. This was measured by asking the respondents the following question: "Have you been the victim of any of the following offences online in the past three years?" The options given were slander or defamation of character, threat of violence, identity theft, sexual harassment, blackmail, consumer fraud, or photos being shared online without permission. With the last question, we wanted to grasp the extent of sexual harassment in Iceland. Of specific interest in the wake of the MeToo confessions in 2017, it is interesting to explore whether these public revelations have any relationship with the sexual victimization experiences reported by women in the 2018 survey. The period under investigation covers three years prior to the survey in 2018 like the first study in 2016. Therefore, in part, the second survey might include victimization experiences occurring during the same time period as the first survey. If respondents had been victims of multiple victimization crime experiences, they could mark more than one crime type.

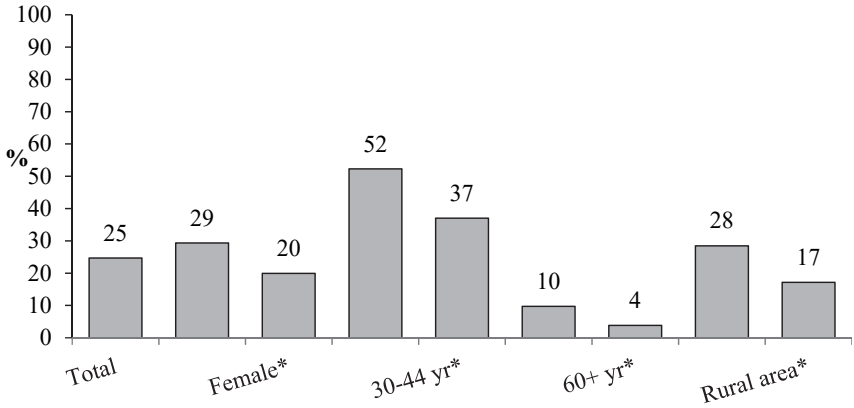
Finally, it was examined how different background variables influenced the likelihood of becoming a victim of online crime. Several different independent variables were included such as gender, age, and residency, i.e., if participants lived in or outside the Reykjavik capital area. Participants were divided into four age groups, 18-29 years old, 30-44 years old, 45-59 years old, and 60 years old and older. Fewer younger members of the panel answered the survey and more participants with university degrees also participated. Therefore, the data had to be weighted for age, gender, education level, and residency to satisfactorily reflect the Icelandic population.

Results

Figure 1 shows the percentage of participants who had illegally downloaded copyrighted material in the past three months prior to the survey. Approximately one-fourth of the participants admitted having done so compared to one-third in 2016. The data showed a significant gender difference, unlike the 2016 findings, with more males admitting illegal downloading in 2018. Difference between age groups was also statistically significant as in 2016. More than half the participants aged 18 to 29 years and more than one-third of respondents aged 30 to 44 years had illegally downloaded copyrighted material compared to only four percent of

participants aged 60 years or older and about ten percent of those aged 45 to 59 years. The difference between participants living in the Reykjavik metropolitan area and those living outside of Reykjavik was also statistically significant. Less than one-third of the residents in Reykjavik and only less than one in five living outside of Reykjavik had illegally downloaded copyrighted material. Apparently, downloading illegally appears to be less frequent in 2018 than in 2016.

Figure 1. Percentage of participants who reported having downloaded copyrighted material in the past three months based on gender, age, and residency

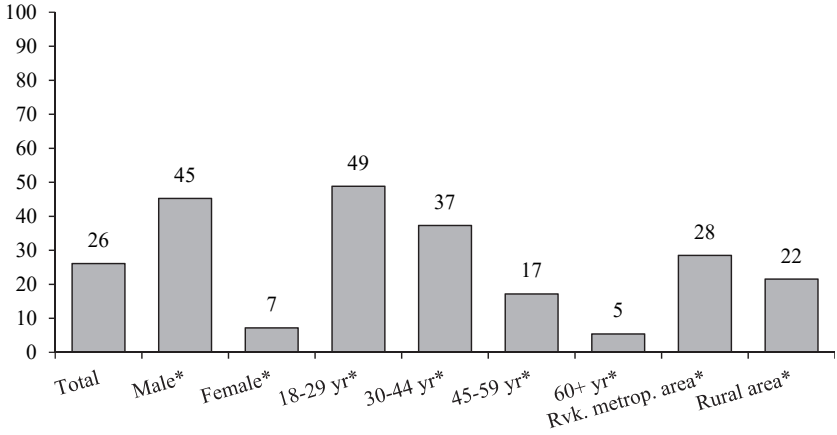


* marks significant difference between groups ($p < 0,05$)

Figure 2 shows the percentage of participants who admitted having visited pornographic websites in the past three months prior to the survey. About one in four Icelanders admitted to having visited pornographic websites during the past three months very similar to 2016. The gender difference was again statistically significant. About 45 percent of males but only 7 percent of females admitted to having viewed pornographic material online in the past three months. It seems that more males and fewer females admit to having visited websites with pornographic material in 2018 than in 2016; thus, the gap between the sexes has apparently widened. There was also a significant difference between different age groups. About half of the younger participants and more than one-third of participants aged 30 to 44 years stated they had visited pornographic websites in the past three months very similar to 2016. Fewer of the older participants admitted to having done so – ap-

proximately 17 percent in the age group 45 to 59 and five percent of respondents 60 years and older. Residency was statistically significant with more residents in Reykjavik admitting to visiting such sites than residents outside the capital area.

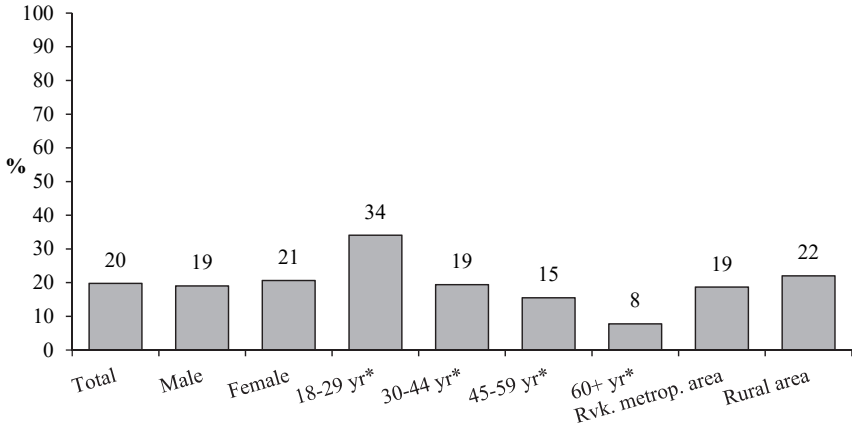
Figure 2. Percentage of participants who had deliberately visited pornographic websites in the past three months, based on gender, age and residency



* marks significant difference between groups ($p < 0,05$)

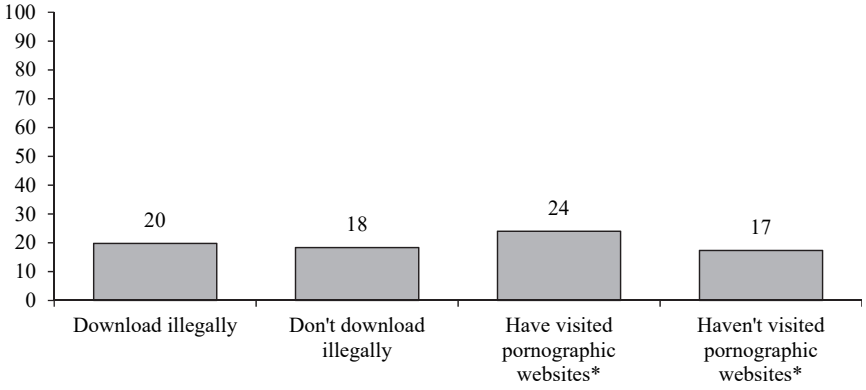
As shown in Figure 3, approximately 20 percent of respondents had been victimized by any of the digital crimes about which we inquired. Gender had no significant impact on digital crime victimization. Age, on the other hand, had a significant influence. As international research has previously shown, digital victimization was highest among the youngest online users. This is different from the 2016 findings in Iceland when the next age group, i.e. those 30 to 44 years old reported highest victimization. Approximately 19 percent of the participants in that age group admitted to victimization but significantly more or 34 percent in the younger group. Fewer of the older participants reported being victimized in the past three years. We did not find a significant difference between those living in the capital area compared to those in rural areas. Approximately 19 percent of the participants living in the Reykjavik area reported being victimized compared to 22 percent of those living outside Reykjavik.

Figure 3. Percentage of participants who reported having been victimized by digital crime in the past three years, based on gender, age and residency



* marks significant difference between groups ($p < 0,05$)

Figure 4. Percentage of participants who reported having been victimized by digital crime in the past three years based on illegal and risky behavior activities online



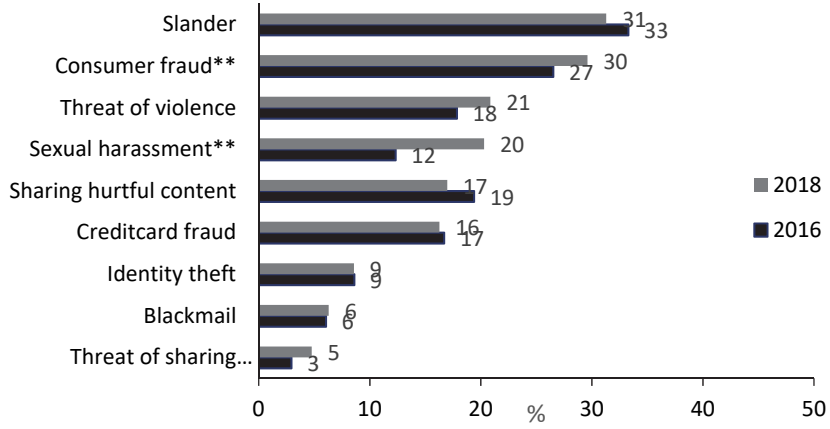
* marks significant difference between groups ($p < 0,05$)

Figure 4 presents digital victimization based on various illegal and risky behavior online. We did not find any statistically significant difference between those who had downloaded illegally and those who had been victimized online. Approximately 20 percent of the participants who had illegally used the internet to stream TV shows, movies or music in the past three months had been victims of some sort of cybercrime compared to about 18 percent of those who did not use the internet to stream. However, there was a significant difference between those who had visited pornographic websites and those who had not. About 24 percent of pornography users but only 17 percent of those who had not visited such sites in the past three months had been victimized. This reflects a change from 2016 when we did not find any statistically significant difference between those who had been victimized and those visiting pornographic websites.

According to the data of the respondents who had been victims of digital crime, slander or defamation of one's character was stated as the most frequent type of crime as shown in Figure 5. Approximately one-third of all victimization experiences consisted of this type of crime which is an outcome very similar to both 2016 and 2018. The second most frequently mentioned victimization type in both 2016 and 2018 was consumer fraud, that is, receiving the wrong product or one's credit card being charged without receiving the product. More than a quarter of the offences reported included online consumer fraud. Approximately 17 percent of the offences included credit card fraud, i.e. having one's credit card number stolen and used without permission. Approximately nine percent of the offences included identity theft, that is, misuse of personal data such as one's social security number. Approximately 18 percent of the victim types reported in 2016 and 21 percent in 2018 included being threatened by violence online in the past three years.

The most notable change, however, between the two surveys in 2016 and 2018 concerns sexual harassment. About 12 percent of the offences consisted of sexual harassment online in 2016 but this figure increased significantly to 20 percent in 2018. Approximately three percent had been threatened with sharing of personal data or personal pictures in 2016, which increased to five percent in 2018. Furthermore, close to one in five victim respondents in both 2016 and 2018 reported that someone had shared a picture of them without their permission.

*Figure 5. Percentage of digital crime types reported by victims for a period of three years prior to the surveys in 2016 and 2018**



*it was possible to mark more than one crime
** marks significant difference between groups ($p < 0,05$)

Conclusion

The number of households with internet access has increased drastically in the past few years. Currently, almost every Icelandic household is connected to the internet (Eurostat, 2019). With increased internet use, online victimization, apparently, has also increased. Previous research has shown that roughly 10 percent of internet users in the US have reported to have been victims of online scams or phishing (Norton, 2012). Our data showed that approximately 20 percent of Icelandic internet users had been victimized by digital crime of some sort during the last three years before the survey was conducted in 2018. However, these figures cannot be fully compared because our survey inquired about a wider range of victimization experiences than the US survey.

The figures for the two Icelandic surveys in 2016 and 2018 are comparable. Here, we see an increase in online victimization. Only about 13 percent of respondents admitted to digital victimization in 2016 which increased significantly to 20 percent in 2018. The relative share of each victimization type remained similar except one notable difference. The percentage of sexual harassment victimization experiences increased dramatically, that is, up to a total of 20 percent who reported victimization in 2018 compared to only 12 percent in 2016. This statisti-

cally significant increase of sexual harassment reporting comes mostly from women. In 2016, fewer women admitted to digital victimization than men. In 2018, more women, or 21 percent, admitted to victimization with 19 percent men. Gender difference was not significant statistically. However, it is noteworthy that the percentage of women reporting victimization increased from 12 in 2016 to 21 percent in 2018, while the increase for males was somewhat less from 15 percent to 19 percent.

How can this almost twofold increase in women reporting online victimization and the increase of those reporting sexual harassment be explained? A plausible explanation might have to do with different social circumstances in 2018 compared to 2016. New social movements appeared after 2016 in which experiences of women played a central role. More specifically, a movement linked to MeToo emerged in Iceland in 2017. Women in different professional groups stepped forward in Iceland with stories of sexual harassment they had experienced in their professional life. These women came from different walks of life such as arts, academia, sports, banks, restaurants, immigrants, etc. Thousands of anonymous stories were accumulated and published online (Beck, 2017). Understandably, these confessions created an uproar in the public debate and the sheer volume came as a surprise to many. A social revolt against sexual discrimination became prominent in Icelandic public life and social awareness of this behavior both increased and deepened. Possibly, this movement has something to do with how many more women came forward in our study in 2018 admitting to digital victimization, especially sexual harassment. Not necessarily reflecting an actual increase for this type of victimization but perhaps suggesting more social awareness among women with respect to recognizing certain unwanted behavior as sexual harassment than before. Harassing communications previously perceived as nothing more than a nuisance, increasingly being interpreted more as sexual harassment in the aftermath of MeToo. However, this aspect needs to be explored further in new studies.

The MeToo confessions might also be linked to why fewer women admit to visiting pornographic websites in 2018 compared to 2016. In 2016, a total of 12 percent of the women admitted to this use during the last three months before the survey was conducted; this dropped to seven percent in 2018. Thus, this behavior is probably not as accepted anymore among women following the MeToo movement, pornography being considered more as a sexist expression of male dominance and sexual objectification of women. Interestingly, this shift in behavior toward pornographic material apparently did not have the same impact on males and their use of porn online. Their use of porn online increased markedly

instead from 39 percent admitting to visiting pornographic websites in 2016 to 45 percent in 2018.

About one-fourth of the participants admitted to having downloaded copyright material illegally compared to one-third in 2016. The data showed a significant gender difference, unlike the 2016 findings, with more males admitting illegal downloading in 2018. Probably more legal access to websites such as Netflix and Spotify explain this downward trend in illegally downloading material.

The lifestyle routine activity theory (RAT) appears to have some relationship with digital crime in Iceland. In 2016, illegal downloading was found to be related to digital victimization. Yet in 2018 we did not find this relationship. However, in 2018, more respondents who had visited pornographic websites admitted to digital crime victimization than others. Therefore, as Holt and Bossler (2008) have previously shown, we found some support of RAT. Risky behavior online seems to be correlated with digital crime victimization, at least in part. Engaging in deviant lifestyles online may expose individuals to motivated offenders, thereby increasing the risk of victimization. More online activity, especially online visits of pornographic sites, tends to increase online victimization according to this study.

The findings also clearly demonstrate the need for including gender in the analysis of cybercrime victimization, especially online harassment. In 2020, our survey measuring online victimization experiences in Iceland, is planned to be conducted for the third time. With a time period of three different years; 2016, 2018 and 2020, gives us a broader reference to examine the trend in cybercrime victimization in general and the true nature of these experiences. Of specific interest is the possible impact of the MeToo movement in Iceland. Was the increase in online sexual harassment reported by women in our 2018 survey just temporary, even coincidental, or will we see the trend continue? What is the nature of the link between MeToo activism and gender based online violence experienced and reported by women? Further research is clearly needed to fully grasp the consequences of the MeToo confessions. Equally important is to update regularly the nature and volume of online crime and victimization experiences in general.

References

Beck, B.H. (2017). Tími þagnarinnar liðinn – sögurnar allar (Time of silence has passed – all the stories included here). Kjarninn. Retrieved from https://kjarninn.is/skyring/2017-12-11-konur-islandi-segja-fra-kynferdisofbeldi-areitni-og-kynbundinni-mismunun-sogurnar-allar/

Bernharðsdóttir, B. (2019). Víða vandi vegna stafræns ofbeldis og nektamynda (Widespread concern about digital violence and nude photos). Visir.is. Retrieved from https://www.visir.is/g/2019191028818/vida-vandi-vegna-stafraens-ofbeldis-og-nektamynda

Buzzell, T., Foss, D., & Middleton, Z. (2006). Explaining use of online pornography: A test of self-control theory and opportunities for deviance. Journal of Criminal Justice and Popular Culture, 13(2), 96-116.

Eurostat. (2019). Digital economy and society statistics – households and individuals. Luxembourg: Publications Office of the European Union. Retrieved from https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals

G Data Securitylabs. (2015). G Data Securitylabs Malware Report: Half-year report January-June 2015. Bochum: G Data Software Inc.

Glaeser, E.L., & Sacerdote, B. (1999). Why is there more crime in cities? Journal of Political Economy, 107, S225-S258. https://doi.org/10.1086/250109

Harder, S.K., Jörgensen, K.E., Gårdshus, J.P. & Demant, J. (2020). In Heinskou, M.B., Skilbrei, M.L., & Stefansen, K. (eds.) (2020). Rape in the Nordic countries: Continuity and change (pp. 205-223). Routledge Research in Gender and Society. https://doi.org/10.4324/9780429467608-13

Harrell. (2015). Victims of identity theft, 2014. Washington: Bureau of Justice Statistics.

Herring, S.C. (1999). The rhetorical dynamics of gender harassment online. The Information Society. 15(3), 151-167. https://doi.org/10.1080/019722499128466

Holt, T.J. and Bossler, A.M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior, 30(1), 1-25. Accessed December 12, 2019: https://www.tandfonline.com/doi/full/10.1080/01639620701876577. https://doi.org/10.1080/01639620701876577

IIE (2019). Retrieved from https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.

Jónasson, J.O. and Gunnlaugsson, H. (2016). How widespread is cybercrime? Types and volume of public victimization in Iceland. In a seminar report from the Nordic Research Council for Criminology (Nordisk Samarbeidsråd for Kriminologi) in Bifröst, Iceland, May 1-4, 2016: 446-457.

Landsbankinn Homepage. (2019). Aldrei meira tjón af netglæpum (Loss due to digital crime at a historic high). Retrieved from https://umraedan.landsbankinn.is/umraedan/samfelagid/verum-vakandi/netglaepir/

Leukfeldt, E.R. & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior, 37(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Marcum, C.D., Higgins, G.E., & Ricketts, M.L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. Deviant Behavior, 31, 381-410. https://doi.org/10.1080/01639620903004903

McGuire, M., & Dowling, S. (2013). Cybercrime: A review of the evidence – Research report 75. London: Home Office.

National Center for Education Statistics (2019). Indicators of school crime and safety: 2018 APRIL 2019. Retrieved from https://nces.ed.gov/pubs2019/2019047.pdf.

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: A multi-nation study. Journal of Scandinavian Studies in Criminology and Crime Prevention, 16(2), 203-210. https://doi.org/10.1080/14043858.2015.1046640

Näsi, M., Räsänen, P., Oksanen, A., Hawdon, J., Keipi, T., & Holkeri, E. (2014). Association between online harassment and exposure to harmful online content: A cross-national comparison between the United States and Finland. Computers in Human Behavior, 41, 137-145. https://doi.org/10.1016/j.chb.2014.09.019

Norton. (2012). Norton cybercrime report 2012. Retrieved from http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf.

Norton. (2016). Norton cybersecurity insights report. Retrieved from https://us.norton.com/norton-cybersecurity-insights-report-global.

Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. Vulnerable Children and Youth Studies, 8(4), 298-309. https://doi.org/10.1080/17450128.2012.752119

Parliamentary Assembly. (2019). Promoting parliaments free of sexism and sexual harassment. Report. Council of Europe. Retrieved from http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-en.asp?FileID=27477&lang=en

Patchin, J.W. & Hinduja, S. (2016). Bullying today: Bullet points and best practices. Thousand Oaks, CA: Sage Publications. https://doi.org/10.4135/9781506335957

Pratt, T.C., Holtfreter, K., & Reisig, M.D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. Journal of Research in Crime and Delinquency, 47, 267-296. https://doi.org/10.1177/0022427810365903

Reyns, B.W., & 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. Retrieved from http://ijo.sagepub.com/content/early/-2015/02/26/0306624X15572861-.refs#cited-by.

Siegel, L.J. (2018). Criminology: Theories, patterns and typologies (13th edn.). Boston: Cengage Learning.

Sigurvinsdóttir, R., Ásgeirsdóttir, B.B. & Arnalds, S. (2020). Breaking the silence: Social media disclosures of sexual violence in Iceland. In Heinskou, M.B., Skilbrei, M.L., & Stefansen, K. (eds.) (2020). Rape in the Nordic countries: Continuity and change (pp. 224-240). Routledge Research in Gender and Society. https://doi.org/10.4324/9780429467608-14

Sigurðsson, Á.F. (2015). Computer and Internet usage in Iceland and other European countries 2014. Statistical Series – Tourism, transport and IT, 100(1), 1-20.

Staksrud, E., Ólafsson, K., & Livingstone, S. (2013). Does the use of social networking sites increase children's risk of harm? Computers in Human Behavior, 29, 40-50. https://doi.org/10.1016/j.chb.2012.05.026

Taylor, P.A. (2003). Maestros or misogynists? Gender and the social construction of hacking. In Dot.cons: Crime, Deviance and the Identity on the Internet (Jewkes, Y. ed.). Portland, OR: Willan Publishing.

UN Women Broadband Commission (2015). Executive Summary: Cyber Violence Against Women and Girls. A Worldwide Wake-Up Call. A Discussion Paper From the UN Broadband Commission For Digital Development Working Group on Broadband and Gender. Ac-

cessed January 16, 2020: ttps://www.broadbandcommission.org/Documents/reports/bb-wg-gender-discussionpaper2015-executive-summary.pdf

Wolak, J., Mitchell, K.J., & Finkelhor, D. (2006). Online victimization of youth: Five years later. Alexandria: National Center for Missing & Exploited Children. https://doi.org/10.1037/e525892015-001

Yar, M. (2013). Cybercrime and society (2nd edn.). London: Sage.

Ybarra, M.L. (2004). Linkages between depressive symptomatology and Internet harassment among young regular Internet users. Cyberpsychology & Behavior, 7(2), 247-257. https://doi.org/10.1089/109493104323024500 PMid:15140367