Iranian Association of Geopolitical

Geography(Regional Planning)

Summer 2023. Vol 13. Issue 51
ISSN (Print): 2228-6462 - ISSN (Online): 2783-2112
Journal Homepage: https://www.jgeoqeshm.ir/

Research Paper

An Introduction to the Harmful Activities of Cyberspace Communication in Iran's Legal System

Ali Haghjoo[1], Dariush Babaei[*2], Ali Janipour[3]

1. Department of private law, Yasooj Branch, Islamic Azad University, Yasooj, Iran.
2. Assistant Professor of Public law, Yasooj Branch, Islamic Azad University, Yasooj, Iran
3. Assistant Professor of private law, Yasooj Branch, Islamic Azad University, Yasooj, Iran

ARTICLEINFO

PP:411-432

Use your device to scan and read the article online

Abstract

The Internet and social networks, like many other phenomena, have positive and negative consequences, and by planning and raising the level of public awareness, we can take advantage of its positive effects and minimize the negative consequences. The rapid growth of technology and especially the ever-increasing progress in the fields of communication, satellites and the Internet has caused rapid changes in human societies and has had many positive and negative effects. In the meantime, the effects of the Internet and cyberspace in social relations are more than in other fields and have caused many changes and transformations. The purpose of writing this article is to examine the harmful activities of cyber space communication in Iran's legal system. Therefore, the structure of the article has been compiled in 8 sections and each section has several speeches. Also, the examples of harmful activities are specifically given, its components are analyzed and the civil responsibility resulting from it is described in the legal system of Iran.

Keywords: *Cyberspace, Legal System, Defamation, Privacy, Phishing*.

Citation: Haghjoo, A., Babaei, D., & Janipour, A. (2023). **An Introduction to the Harmful Activities of Cyberspace Communication in Iran's Legal System**. Geography(Regional Planning), 13(51), 411-432.
DOI: 10.22034/JGEOQ.2023.327400.3546
DOR: 20.1001.1.22286462.1402.13.51.25.7

[*] **Corresponding author:** Dariush Babaei, **Email:** dr.babaei56@yahoo.com

Extended Abstract

Introduction

The Internet, initially designed for military and security purposes, gradually expanded its presence into various social sectors, including business, recreation, and entertainment. Its diverse and extensive functionalities led to a transformation from a military tool to a global industry, influencing almost every aspect of society. The Internet emerged as a mass media platform in Western countries and, over time, extended its reach globally, becoming an influential tool in disseminating policies, culture, and economic trends. This global shift in the use of the Internet has had profound consequences and impacts on human societies, often referred to as the "information explosion" in communication science and sociology.The Internet's transcendent nature across space and time has given rise to new forms of social interactions, ushering in significant changes in lifestyle, social dynamics, and even political participation. Today, the Internet stands as the primary channel for information dissemination and public communication.This research aims to explore the detrimental activities within cyberspace in Iran's legal framework. To achieve this, the following research questions were formulated:

What are the civil and criminal responsibilities outlined in Iran's press law?

Can you provide examples of media damage, and how is punishment determined within Iran's legal system?

How does the virtual space serve as a tool for warfare?

What instances of copyright and privacy violations occur in cyberspace, and how are they legally addressed in Iran?

What civil liabilities arise from defamation, spreading false information, system hacking, and phishing in Iran's legal system?

Methodology

In this research, a descriptive-analytical research method has been employed to examine and interpret the Iranian legal system and the challenges associated with malicious activities in the cyberspace

Results and Discussion

The imperative of preserving personal privacy is paramount in the digital age, where cyber observers play a pivotal role in either instigating or preventing privacy breaches. Cyber space, with its trans-boundary and temporal nature, reshapes societal interactions, influencing lifestyle, social dynamics, and political participation. Vulnerabilities, lack of virtual environment awareness, and data protection negligence expose individuals to cyber victimization. While emphasizing the importance of safeguarding personal information, this discussion underscores the need for proactive measures in the face of cyber threats. Neglecting cybersecurity leaves individuals susceptible to privacy infringements, highlighting the significance of personal responsibility in thwarting cybercriminal actions (Tazzy, 2012). Compensation for material and moral damages caused by defamation is a legal right. The Civil Liability Law, particularly Article 1, holds individuals accountable for harm to others' reputation. Despite press laws attempting to address these issues, deficiencies remain. Iran's penal laws are considered insufficient, and legal experts find the press law's measures inadequate for remedying reputational damage. Cybercriminals, specifically hackers, engage in information theft through hacking, accessing personal data. Identity theft involves exploiting sensitive information for financial or malicious purposes. Technological advances have positive and negative impacts, with hackers posing threats through unauthorized access and data breaches.

Conclusion

In conclusion, it is evident that the detrimental activities in cyberspace necessitate the amendment and modernization of Iran's legal regulations. The swift impact of technology underscores the need for crafting new laws and enhancing legal frameworks to safeguard

individuals and ensure digital security. International collaboration and extensive cooperation, coupled with legal overhauls, are imperative for addressing cyber challenges and advancing global security.

References

1. Ansari, B. (2008). Communication Law (2nd ed.). Tehran: SAMT Publications. [In Persian]
2. Ansari, B, et al. (2002). Civil Liability of Mass Media. Compilation and Revision of Laws and Regulations. Tehran: Research, Compilation, and Revision of Laws and Regulations Deputy Publications. [In Persian]
3. Aiti, H. (1996). Intellectual Property Law with an Emphasis on Literary and Artistic Rights. Tehran: Hoghooghdan Publications. [In Persian]
4. Regulation for Mandatory Installation and Registration of Trademarks, Approved on 1970/4/13. [In Persian]
5. Bashari Rad, B, & Habibi, A. (2012). Computer Viruses and Malwares. Tehran: Naqoos Publications. [In Persian]
6. Pakzad, Batool. (1996). Computer Crimes. Master's Thesis, Faculty of Law, Shahid Beheshti University. [In Persian]
7. Peter Carey, Jo Sanders. (2007). Media Law. Translated by Hamid Reza Malek Mohammadi. Tehran: Mizan Publications. [In Persian]
8. Dezhiani, M H. (1997). International Criminal Policy Journal, Numbers 33 and 34, Computer Crimes Handbook, Volume 1, Supreme Informatics Council. [In Persian]
9. Faghih Habibi, A, &Safaee Far, A. (2012). Development of Civil Liability in Media and Press Crimes. Journal of Communication Sciences, 9, 22-41. [In Persian]
10. Law on the Procedure of Public and Revolutionary Courts (Criminal Matters).
11. Electronic Commerce Law - Approved in 2003.
12. Law on the Translation and Reproduction of Books, Journals, and Audio Works - Approved in 1973.
13. Law on the Registration of Trademarks and Patents - Approved on 1931/4/1 and the Amendment Regulation for the Implementation of the Trademark and Patent Registration Law - Approved in 1958.
14. Computer Crimes Law - Approved on February 11, 2011.
15. Law on the Protection of the Rights of Authors, Composers, and Artists - Approved in 1969.
16. Press Law - Approved in 1979.
17. Press Law - Approved in 1985.
18. Katozian, N. (1999). Non-Contractual Obligations: Volume Two, Civil Liability. Tehran: University of Tehran Publications. [In Persian]

فصلنامه جغرافیا (برنامه ریزی منطقه ای)

دوره ۱۳، شماره ۵۱، تابستان ۱۴۰۲

شاپا چاپی: ۶۴۶۲- ۲۲۲۸ شاپا الکترونیکی: ۲۱۱۲ -۲۷۸۳

Journal Homepage: https://www.jgeoqeshm.ir/

انجمن ژئوپلیتیک ایران

مقاله پژوهشی

مقدمه‌ای بر فعالیت‌های زیان‌بار ارتباطات فضای سایبری در نظام حقوقی ایران

علی حق‌جو- گروه حقوق خصوصی، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران.

داریوش بابایی[*]- استادیار گروه حقوق عمومی، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران

علی جانی پور- استادیار گروه حقوق خصوصی، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران

اطلاعات مقاله

شماره صفحات: ۴۳۲-۴۱۱

از دستگاه خود برای اسکن و خواندن مقاله به صورت آنلاین استفاده کنید

واژه‌های کلیدی:

فضای سایبری، نظام حقوقی، هتک حرمت، حریم خصوصی، فیشینگ..

چکیده

یکی از مشخصات تغییرات سریع دنیای امروز فناوری ارتباطات و اطلاعات است که شتاب تغییرات را در همه بخش‌های زندگی رقم‌زده است. بااین‌وجود آثار مثبت متعدد فضای مجازی، پیامدهای نامطلوبی نیز رخ داده است که بررسی وضعیت حقوقی آن اجتناب‌ناپذیر است؛ بنابراین، هدف پژوهش حاضر بررسی فعالیت‌های زیان‌بار ارتباطات فضای سایبری در نظام حقوقی ایران است. اینترنت و شبکه‌های اجتماعی مانند بسیاری از پدیده‌های دیگر دارای پیامدهای مثبت و منفی می‌باشد که با برنامه‌ریزی و بالا بردن سطح آگاهی عمومی می‌توان از آثار و دستاوردهای مثبت آن بهره گرفت و پیامدهای منفی را به حداقل رساند. رشد سریع تکنولوژی و به‌ویژه پیشرفت روزافزون در حوزه‌های ارتباطی، ماهواره‌ها و اینترنت باعث تحولات پرشتاب در جوامع بشری گردیده و آثار مثبت و منفی فراوانی در پی داشته است. در این میان، آثار اینترنت و فضای سایبری در روابط اجتماعی بیش از سایر حوزه‌ها بوده و تغییرات و دگرگونی‌های زیادی را به وجود آورده است. هدف از نگارش این مقاله بررسی فعالیت‌های زیان‌بار ارتباطات فضای سایبری در نظام حقوقی ایران می‌باشد؛ بنابراین ساختار مقاله در ۸ بخش و هر بخش در چند گفتار تدوین گردیده است. همچنین به‌طور ویژه مصادیق فعالیت‌های زیان‌بار آورده شده، اجزای آن موردبررسی و تحلیل قرارگرفته و مسئولیت مدنی ناشی از آن در نظام حقوقی ایران تشریح گردیده است.

استناد: حق‌جو، علی؛ بابایی، داریوش؛ جانی‌پور، علی. (۱۴۰۲). **مقدمه‌ای بر فعالیت‌های زیان‌بار ارتباطات فضای سایبری در نظام حقوقی ایران**. فصلنامه جغرافیا (برنامه‌ریزی منطقه‌ای)، ۱۳(۵۱)، صص ۴۱۱-۴۳۲.

DOI: 10.22034/JGEOQ.2023.327400.3546
DOR: 20.1001.1.22286462.1402.13.51.25.7

[*] **نویسنده مسئول:** داریوش بابایی، **پست الکترونیکی:** dr.babaei56@yahoo.com

مقدمه

رشد سریع تکنولوژی و بویژه پیشرفت روزافزون در حوزه‌های ارتباطی، ماهواره‌ها و اینترنت باعث تحولات پرشتاب در جوامع بشری گردیده و آثار مثبت و منفی فراوانی در پی داشته است. در این میان، آثار اینترنت و فضای سایبری در روابط اجتماعی بیش از سایر حوزه‌ها بوده و تغییرات و دگرگونی‌های زیادی را بوجود آورده است.

اینترنت که ابتدا برای اهداف نظامی و امنیتی طراحی شده بود، به مرور وارد دیگر بخش‌های اجتماعی ازجمله تجارت، تفریح و سرگرمی و ...گردید و این امر چنان پر رنگ و گسترده بود که کارکرد آن را تغییر داد بطوری‌که این تکنولوژی نوظهور، امروزه به یک صنعت و عرصه‌ی تاثیرگذار جهانی تبدیل شده است و کمتر موضوع اجتماعی را می توان یافت که متاثر از اینترنت نباشد. اینترنت ابتدا در کشورهای غربی به عنوان رسانه‌ای همگانی رواج یافت و بتدریج دیگر کشورها را نیز در بر گرفت و به مثابه ابزاری موثر در انتقال و ترویج سیاست‌ها، فرهنگ، اقتصاد و ... کاربرد پیدا کرد. این تغییر و تحولات جهانی و گرایش همه جانبه به استفاده از اینترنت، تبعات و تاثیرات بسیاری در جوامع بشری داشت تا جایی که از آن به «انفجار اطلاعات» تعبیر می‌شود و مفهومی پر کاربرد در علم ارتباطات و جامعه شناسی است.

فرا مکان و فرا زمان بودن اینترنت و در دسترس بودن آن، موجب شکل‌گیری شیوه جدیدی از تعاملات اجتماعی نسبت به گذشته شد و تغییراتی شگرف در سبک زندگی، تعاملات اجتماعی و حتی مشارکت سیاسی و نحوه آن به وجود آورد تا جایی که امروزه اینترنت بیشترین نقش را در اطلاع‌رسانی و تبلیغات برای عموم دارد و به عنوان اصلی‌ترین کانال ارتباطی محسوب می‌شود. پژوهش حاضر با هدف بررسی فعالیت‌های زیانبار ارتباطات فضای سایبری در نظام حقوقی ایران انجام شد، بدین منظور سوالات پژوهش بصورت ذیل طرح گردید:

– مسئولیت مدنی و کیفری در قانون مطبوعات ایران چیست؟
– مصادیق آسیب‌های رسانه‌ای کدامند و مجازات تعیین شده در نظام حقوقی ایران چگونه است؟
– فضای مجازی چگونه ابزار را برای جنگ ایجاد می‌کند؟
– مصادیق نقض کپی رایت و حریم خصوصی در فضای سایبری کدامند و حکم آن در نظام حقوقی ایران چیست؟
– مسئولیت مدنی ناشی از هتک حرمت، اشاعه‌ی اکاذیب، هک سیستم و فیشینگ در نظام حقوقی ایران چیست؟

مبانی نظری

مسئولیت توأمان مدنی و کیفری در قانون مطبوعات ایران

مسئولیت کیفری رسانه‌ها و مطبوعات در نظام حقوقی ایران توأم با مسئولیت مدنی و مطالبه ضرر و زیان ناشی از جرم می‌باشد. شخص می‌تواند جبران خسارت خود را ضمن مجازات کیفری تقاضا نماید؛ اما بنظر می‌رسد مسئولیت توأمان کیفری و مدنی به معنای یکسانی جرم در جرائم مطبوعاتی نیست بلکه جرم مطبوعاتی تفاوت‌هایی دارد ازجمله در جزای عمومی قصد مجرمانه شرط است که در مطبوعات حاصل اصلی تحقق خارجی جرم است.

بنابراین با لحاظ این مسئولیت نمی‌توان در همه موارد این گونه قضاوت کرد. بر این اساس رویه قضایی تاکنون در حوزه مطبوعات چنین بوده که اگر فرد مسئولیت کیفری مدیران مطبوعات را هدف گرفته دادگاه در رسیدگی فقط بدان توجه داشته است و موردی سراغ نداریم که همزمان و توأمان مسئولیت کیفری و مدنی را مورد حکم قرارداده باشد، گرچه در قالب رسیدگی کیفری جریمه با جزای نقدی حکم کرده‌اند اما پرداخت خسارت در حق مدعی تاکنون سابقه نداشته است چنانچه مدعی بر اساس مسئولیت مدنی رسانه مطبوعات اقدام نموده نیزدادگاه فقط به همین مسئله توجه داشته است و نسبت به آن حکم به خسارت صادر نموده و مجازات کیفری رها شده است.

از سوی دیگر مسئولیت مدنی در حقوق مطبوعات به دلیل شرایط خاص رسانه ضرورت نظام مدرن رسانه‌ای متفاوت با نگرش سنتی به مسئولیت مدنی است لیکن ابزار مسئولیت مدنی یا ویژگی انعطاف‌پذیری و قابلیت تطبیق آن در موارد متعدد از برجستگی و قوت آن است که در حقوق رقابت مدرن و توسعه بخش‌های اقتصاد جهانی به خوبی می‌تواند از عهده آن برآید. حال آنکه مسئولیت کیفری و اصل قانونی بودن جرم و مجازات ضرورت تصریح قانون به فعل مجرمانه از عواملی است که در حوزه مطبوعات

ممکن است در انطباق با مشکل مواجه شوید؛ بنابراین تمایل درونی و اقتضاء رسیدن به حق شهروندان تأکید بر مسئولیت مدنی و پرداختن بدان است اما روش شروع به پیگیری در سیستم قضائی به طور سنتی افراد را به سوی شکایت کیفری می‌کشاند.

مسئولیت مدنی رسانه‌ها درایران

مسئولیت مدنی در تمامی امور زندگی بشرامروزجریان دارد. به ویژه با تخصصی شدن مشاغل و حرف مسئولیت از اهمیت بیشتری برخوداراست؛ بنابراین ازدیدگاه حقوقای ایران مسئولیت مدنی بر ۱- وجود ضرر،۲- فعل عامل زیان و ضرر،۳- وجود رابطه سببیت یا علیت بین زیان حاصله و فاعل زیان.

درصورت تحقق این شروط باید جبران خسارت شود مطبوعات و رسانه نگاران نیزدرایفای نقش ومسئولیت خویش ممکن است عملی مرتکب شوند که باعث ضرر و زیان به شخص یا اشخاص شوند و این می تواند زمینه مسئولیت مدنی رسانه باشد.

بی‌تردید درصورتی که مدعی ورود خسارت به خود بتواند ثابت نماید که عمل روزنامه باعث ضرر مادی یا معنوی به وی شده است و ارکان آن را به اثبات برساند بدون تردید رسانه موظف به جبران خسارت می گردد؛ اما سؤال مهم این است که چه عملی موجب مسئولیت مدنی است نظریات طرح شده در حوزه مسئولیت مدنی عام است ونسبت به رسانه و مطبوعات نیز از همان ویژگی برخوردار است فقط انگیزه شرافتمندانه اهل قلم یک رکن اصلی تعیین کننده حمایت از آنان دردادرسی است.

نظریه تقصیر

تقصیر از مهم‌ترین عناصر مسئولیت مدنی است که از دیرباز تا امروز مطرح است و قانون م .م در ایران نیز این نظریه را اصل پنداشته است. عدول و فراتر رفتن از حدود متعارف نسبت به هر عملی را می‌توان تقصیر دانست عناصر سه گانه مادی، قانونی ومعنوی در هر فعلی لازم است. انجام فعل مادی مطبوعاتی که عمل مثبت و زیانبار است وعنصر قانونی نیز در قانون مطبوعات یا مجازات اسلامی است، عنصرمعنوی عدم رعایت نظامات، بی احتیاطی، بی مبالاتی، عدول ازحدود متعارف می تواند عنصر معنوی تقصیر باشد. البته فعل زیان آور باید قابل استناد به خوانده باشد و موضوع آن متقابلاً نسبت به مدعیه مقابل صدق باشد. تقصیر می تواند قابل اغماض باشد چنانچه اثر جدی برآن بار نشود و یا عرف آن را جدی نپندارد و قابل گذشت بداند جزیی است، ولی تقصیر سنگین قابل گذشت نیست و عرف هم آن را دارای ابعاد تأثیرگذار می‌داند لذا هر کجا تقصیر سنگین باشد به قاعده قابل گذشت نیست، این تقصیرنوعی است. زیان دیده از تخلف روزنامه لازم نیست که به موادقانونی یا «ب .م .م» و مطبوعات اشاره کند چون رویه قضایی و تشخیص قاضی با استناد به ماده ۸«ب .م .م» مطبوعات ۱۳۶۴ نسبت به صدور حکم و در صورت لزوم جبران خسارت اقدام می نماید. درقانون ایران اصل برتقصیراست و رویه قضایی نیز به تقصیر گرایش دارد.

نظریه ایجاد خطر

بوجودآورنده زمینه کاری که ممکن است منجر به خطراتی شود همانگونه که ازسود و مزایای آن برخورداراست باید مسئولیت زیان آوربودن وخطر ایجاد شده را نیزبپذیرد

این مسئله صرفاً درمورد کارخانه یا مؤسسه تولیدی نیست هر کاری و ازجمله مطبوعات ورسانه هامی توانند درذیل همین مفهوم قرار بگیرند. بر این اساس برای مدیرمسئول فرض تقصیرمی شود وازنظرقانون «م .م» ایران مسئولیت برای دارنده حق امتیاز قطعی ومسلم فرض می شود درحقوق مسئولیت مدنی فرانسه نیز همین مسئله صادق است. چنانچه رسانه با تبلیغات خود از کالایی موجبات تخریب دیگری را فراهم آورد و به او زیان و خسارتی وارد نماید مسئول است. چنان که در تبلیغات انتخاباتی می‌توان به همین نظریه توسل جست وروزنامه نگاریا رسانه خاطی را مورد مؤاخذه قرارداد. البته نحوه ثبوت واثبات خطرمراحلی دارد که باید برطبق قواعد عام مسئولیت مدنی تطبیق صورپذیرد (فقیه حبیبی و صفایی فر، ۶:۱۳۹۱).

آسیب‌های رسانه ای

در خصوص رسانه‌ها می بایست ضررهای مادی یا معنوی را برطبق مصادیق مربوطه تعیین نمود. فرضاً چنانچه کسی حق انتشار یک اثر ادبی را که برای نویسنده آن است، بدون وجود مجوز منتشر نماید موجبات ورود ضرر به نویسنده را فراهم نموده و یا اگر شخصی در قالب یک گزارش رسانه ای محصول کارخانه ای را غیر بهداشتی اعلام نماید عملاً موجب زیانکارخانه تولیدکننده محصول مربوطه گردیده است و یا چنانچه روزنامه، نشریه، رسانه صوتی و تصویری علیه شخصی اعم از حقیقی یا حقوقی، عمومی یا خصوصی هجو نامه ای منتشر نماید؛ موظف به جبران زیان وارده به متضرر است که قوانین مختلف در این راستا مؤید موضوع است در شرع نیز جبران ضرر واجب است و ضرر ناشی از فعل مجنون و نائم نیز ضمان آور چه رسد به اصحاب رسانه که از فرهیختگان جامعه اند. بعضی از اقدامات رسانه ها در ورود ضرر و زیان به اغیار با توجه به نحوه فعالیت و قوانین حاکم مجرمانه بوده و قابلیت مجازات دارد. بدیهی است مجازات مرتکب خود یکی از راهکارهای آرامش روحی و عاطفی زیان دیده است ازجمله مجازات های کیفری و یا جبران خسارت حقوقی قابل اعمال در رسانه های گروهی باید منطبق با نوع جرم و نوع فعل و نوع رسانه مرتکب جداگانه مورد بررسی قرار گیرد. اعمال زیانبار رسانه ها در ورود ضرر مادی یا معنوی به دیگری بعضاً در قالب موارد ذیل واقع می شود.

نقض حریم خصوصی

در نظام حقوقی ایران اصول ۲۲، ۲۳ و ۲۵ قانون اساسی و مواد ۵۷۰، ۵۸۰ و ۵۸۲ قانون مجازات اسلامی به برخی از مسائل مربوط به حریم خصوصی اشخاص توجه نموده اند چراکه هرکس غیر از خود شخص هیچ حقی به ورود به قلمرو درون خویش را ندارد. اصل ۲۲ قانون اساسی: حیثیت، جان، مال، حقوق مسکن و شغل اشخاص از تعرض مصون است مگر در مواردی که قانون تجویز کند- .اصل ۲۳ قانون اساسی: تفتیش عقاید ممنوع است و هیچ کس را نمی توان به صرف داشتن عقیده ای مورد تعرض و مواخذه قرار دارد. اصل ۲۵ قانون اساسی: بازرسی و نرساندن نامه ها ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابرات و نرساندن آنها، استراق سمع و هرگونه تجسس ممنوع است مگر به حکم قانون.

هتک حرمت

در تحقق هتک حرمت باید دو شرط علنی بودن که در رسانه های همگانی با پخش و انتشار محقق می شود و نیز معین بودن شخص مورد هتک که اعم از شخص یا گروهی قابل شناسایی است لحاظ گردد پیشرفت های روزافزون علمی و فنی دنیای نوین بویژه در عرصه رسانه‌های همگانی باعث شده که زندگی خصوصی هر روز مورد تهدید قرار می‌گیرد امروزه اطلاعات به منزله کالای جدید است که می تواند دنیا را تکان دهد هتک حرمت عمدتاً در رسانه ها در قالب افترا (انتساب صریح عمل مجرمانه به غیر و عدم توانایی به اثبات آن) و توهین (انتساب صریح عمل مجرمانه به غیر و عدم توانائی به اثبات آن) و توهین انتساب هرامر وهن آوری اعم از دروغ یا راست به هر وسیله و روش با ترکیب سه عنصر وهن آور بودن مطلب منتسبه و انتشار و پخش آن و علم به وهن آور بودن آن و نشر اکاذیب (انتساب موضوع مورد انتشار و پخش به زیان دیده) تجلی می یابد که برای ارتکاب این افعال در قانون مجازات اسلامی مجازات تعیین گردیده هرکس به هر وسیله‌ای (چاپی-خطی-روزنامه-جرائد-نطق در مجامع یا هر وسیله دیگر...) جرمی را به کسی منتسب بداند ولی نتواند ثابت کند یا به قصد اضرار یا تشویش اذهان عمومی اوراق چاپی یا خطی بدون امضاء یا با امضاء را برخلاف حقیقت ارسال کند علاوه بر اعاده حیثیت و جبران ضرر مادی و معنوی به حبس محکوم می گردد.

در خصوص انتشار گفتارهای توهین آمیز از طریق شبکه‌های الکترونیکی و اینترنت برخی معتقدند که همانند برنامه های رادیو و تلویزیون بوده و بر همین اساس بایستی آن‌ها را در دسته هتک حرمت های گذرا تلقی نمود، اما برخی دیگر نظر مخالف دارند.. یک پیامی که در صفحه یک سایت اینترنتی قرار دارد قطعا به صورت گذرا نبوده و با توجه به گستردگی خدمات دسترسی اینترنت، قابل رویت برای میلیون ها نفر در سراسر جهان خواهد بود. از این رو چه بسا اثرات سوء ناشی از هتک حرمت در فضای الکترونیکی بیش از نشریات و روزنامه‌ها ی غیرالکترونیکی یا حتی برنامه های رادیو و تلویزیون است. نخستین عنصر ضروری برای تحقق

هتک حرمت و ایجاد مسوولیت عبارت است از این که یک اظهار توهین آمیزی که موجب هتک حرمت شخص شود، وجود داشته باشد. این رکن در واقع خود مبتنی بر دو قسمت و شرط ضروری است. اولا اظهار صورت گرفته بایستی خلاف واقع باشد. ثانیا توهین آمیز باشد. لذا چنان چه اظهار صورت گرفته یااظهار واقعیت باشد مسوولیتی متوجه اظهار کننده نخواهد بود، مگر در صورتی که موجب نقض حریم خصوصی اشخاص شود (انصاری و همکاران، ۱۳۸۱).

گمراه کردن از طریق تبلیغات

رسانه ها قادرند با تبلیغات امر موهومی را صحیح و امر صحیح و مقبولی را موهوم جلوه دهند ارائه تبلیغات غیرصحیح در عرصه های مالی (تجاری) یا فرهنگی یا سیاسی (انتخاب ریاست جمهوری، مجلس، خبرگان، شوراهای شهر و روستا) همگی امکان تحقق ضرر را دارد رسانه نباید در هر یک از این عرصه ها از قواعد و مقررات حاکم بر موضوع خارج شود و یا با آگهی تبلیغاتی مقایسه ای درصدد تخریب. باشد.

تحریک به جرائم علیه امنیت

رسانه ها درصورت اقدام به تحریک مردم یا گروه خاص به اقدام علیه امنیت می بایست مسئولیت ناشی از اقدام خویش را بپذیرند در این راستا ماده ۲۵ قانون مطبوعات مجازات کیفری را به قانون مجازات عمومی سابق احاله داده و مفاد ماده ۵۱۲ و ۵۰۴ قانون مجازات اسلامی نیز در خصوص موضوع تعیین تکلیف نموده است لیکن براساس عمومات قانونی و قواعد مختلف فقهی موجود مسئولیت مدنی ناشی از اقدام رسانه نیز قابلیت توجه دارد. اقدام به تحریک علیه امنیت دارای مصادیق متعدد و بی پایانی است که از آن جمله تبلیغ علیه جمهوری اسلامی، تحریک به شورش در نیروهای مسلح و ایجاد تحریکات قومی و قبیله‌ای نیز هست.

انتشار اسناد محرمانه دولتی و نظامی

انتشار اسناد محرمانه و سری دولتی بموجب قانون مجازات جرائم نیروهای مسلح و قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی مصوب ۱۳۵۳ غیرمجاز و مستوجب عقوبت است که اسناد محرمانه و سری و... دارای آئین نامه مخصوص است که تمامی رسانه‌ها از انتشار این گونه اسناد و بدون مجوز قطعاً ممنوع خواهند بود و چنانچه در راستای ارتکاب این فعل زیان به شخص، گروه و یا حتی دولت وارد گردد موظف به جبران زیان خواهند بود در سالهای اخیر نیز چاپ سند محرمانه وزارت اطلاعات در روزنامه سلام موجب تعطیلی این روزنامه و برخورد جزائی با مدیر مسئول آن شد.

نشر اکاذیب

دروغ پراکنی در تمامی ادیان و سیستم های حقوقی قبیح و جرم است در ماده ۶۹۸ قانون مجازات اسلامی هرکس به قصد اضرار دیگران یا تشویش اذهان عمومی یا مقامات رسمی یا شکوائیه یا... یا توزیع اوراق چاپی یا خطی با امضاء یا بدون امضاء اکاذیبی را اظهار نماید. باید به حبس از دو ماه تا دو سال و یا هفتاد و چهار ضربه شلاق محکوم شود و بند ۱۱ ماده ۶ قانون مطبوعات مصوب سال ۷۹ نیز پخش شایعات و مطالب خلاف واقع و یا تحریف مطالب دیگران را جرم دانسته و در تبصره این ماده مجازات های مقرر در ماده ۶۹۸ را برای متخلف در نظر گرفته و اصرار در ارتکاب را نیز موجب لغو پروانه اعلام نموده است بنابر این بر اساس عمومات قانون مسئولیت مدنی متضرر از جرم حق مطالبه خسارت را نیز خواهد داشت (پیتر کری، ۱۳۸۶).

دعوت به خودکشی

مطابق با ماده ۱۵ ق.ج.ر، دعوت به خودکشی از طرق سامانه های رایانـه ای، مخـابراتی و حاملهای داده، جرم است که مصادیق آن در عرف عـام و خـاص، قابـل شناسـایی اسـت، هرچند که به نظر میرسد وسیله موضوعیت دارد ولی شایسته آن بود که قانون‌گذار، دعوت به خودکشی را محدود به استفاده از این ابزار نمیکرد زیرا وقتی با تماس تلفنی، دعوت بـه خودکشی جرم است، به طریق اولی بدون استفاده از تلفن هم اگر دعوت به خودکشی شود، باید جرم باشد.

در دعـوت بـه خودکشـی، روش خودکشـی موضـوعیت نـدارد و فرقـی نمـیکنـد کـه خودکشی با روش موردنظر دعوتکننده محقق شود یا خیر، زیرا واژۀ دعـوت اطـلاق دارد و مقید به انجام روش خاصی نشده است. دعوت، هم بهصورت شفاهی امکانپـذیر اسـت و هم بهصورت کتبی، اما آنچه مهم است، صراحت دعوت است. دعوت به خودکشی متمایز از پیشنهاد به خودکشی است زیرا درمورد اخیر، صراحتی وجود ندارد. برگشـت از دعـوت نمیتواند موجب زوال جرم شود زیرا این جـرم، آنـی اسـت کـه عنصـر مـادی اش در یـک لحظه واقع شده اسـت. بـا توجـه بـه تعریـف «مخاطـب» در بنـد «ج» مـاده ۲ قـانون تجـارت الکترونیکی (۱۳۸۲)، دعوت باید به مباشرت انجام شود، نه اینکه فردی دیگـر واسـطه قـرار گیرد، مگر اینکه عین مفـاد دعـوت بـا اسـتفاده از ابزارهـای مـذکور در قـانون، بـه شـخص مذکور انتقال داده شود، به‌طوری که متن منتسب به دعوتکننده باشد. دعـوت شـونده بایـد مورد خطاب قرار گیرد و لزوماً باید معـین باشـد هرچنـد کـه اشـتباه در هویـت، تـأثیری در ماهیت جرم ندارد. دعـوت بـه خودکشـی مقیـد بـه نتیجـه نیسـت، هرچنـد بـرای تحقـق آن سوءنیت خاص ضروری است. دعوت مشروط نیـز بـه دلیـل اینکـه جـرم، مقیـد بـه شـرط و نتیجه‌ای نیست، واقع میشـود. امـا دعـوت بـه امـر محـال، دعـوت بـه خودکشـی محسـوب نمی‌شود زیرا چنین دعوتی حاکی از عدم قصد اسـت. درصـورتی کـه دعـوت شـونده طفـل غیرممیز یا مجنون باشد، دعوتکننده سبب اقـوی از مباشـر محسـوب مـی شـود. دعـوت بـه خودکشی از نظریه مجرمیت مستقل تبعیت میکند زیـرا مـاده ۱۵ ق. ج. ر بـرخلاف مـاده ۱۲۶ ق. م. ا (۱۳۹۲) تبصره‌ای در رابطه با وحدت قصد ندارد و در ایـن مـاده، ایـن جـرم بـه تحقق خودکشی موفق یا ناموفق منوط نشده است. دعوت به خـودزنی در صـورتی دعـوت به خودکشی محسوب میشود که دعوت شونده، دعوت به وارد کردن ضـربه کشـنده‌ای بـه خود شده باشد. دعوت به خودکشی اگر دو یا چند طرفه باشد و بـا اسـتفاده از سـامانه‌هـای رایانه‌ای، مخابراتی و حاملهای داده انجام پذیرد، پیمان خودکشی محسوب و جـرم اسـت، هرچند طرفین، پس از بستن پیمان منصرف شوند (شاکری و رستگاری، ۱۳۹۲).

چالش نهنگ آبی

بازی نهنگ آبی اولین بار حدود چهار سال پیش در یک شبکه اجتماعی روسی به نام وی کی» آغاز شد. این شبکه اجتماعی که چیزی شبیه به فیس‌بوک است، کاربرانش در کشورهای روسیه، اوکراین، مولدوای و قزاقستان را با ترفندهای خاصی به انجام مراحل غیرعادی این چالش تشویق می‌کرد و درنهایت از آنها می‌خواست تا به زندگی خود پایان دهند.

در این چالش اینترنتی ۵۰ مرحله‌ای، برای هر کاربر یک راهنما وجود دارد که از کاربر می خواهد به ۵۰ چالش به شکل تدریجی عمل کند. بعد از انجام هر مرحله راهنما می خواهد کاربر که عمدتا نوجوان است عکسی از اقدام خود ارسال کند تا وارد مرحله بعدی شود. مرحله نخست این چالش کشیدن یک نهنگ آبی روی دست است و پس از آن مرحله به مرحله بازی خشونت بیشتری پیدا می‌کند برای مثال از کاربر خواسته می‌شود تا لب خود را ببرد، روی دست خود با چاقو کلمه‌ای را حک کند و یا بالای یک ساختمان مرتفع با پاهای آویزان از خود عکس بیاندازد. در مرحله آخر که چالش ۵۰ است از کاربر خواسته می‌شود خود را بکشد.

جنگ نرم و فضای مجازی

استفاده از فضای مجازی ابزاری است برای ورود به جنگ نرم؛ زیرا نظام سلطه برای تحمیل اراده خود به جای استفاده از ابزارهای سخت افزارانه، جنگ نرم را با ایفای نقش ماهواره و اینترنت برای اشغال کشورها در دستور کار قرار داده است، به نحوی که ناکامی آمریکا در جنگ سخت و پرهزینه بودن آن، سبب تغییر رویکرد گردیده است. فضای سایبر یا فضای مجازی به عنوان کلید محیط الکترونیکی است که ارتباط افراد انسانی را با تکیه بر ابزارهای خاص الکترونیکی مخابراتی به صورت آسان و سریع برقرار می‌سازد. این محیط با کارویژه‌های معین خویش، بستر مناسبی را برای پیگیری و تبیین آنچه امروز به جنگ نرم مشهور است ایجاد می‌نماید. توانایی فضای سایبر در کنترل و هدایت منازعات نرم باعث شده است، کشورهای سلطه گر حسابی ویژه را برای نقش آفرینی این براندازی (داخلی) در محیط مجازی در نظر بگیرند. به گونه‌ای که امروز عمده‌ترین ابزار هدایت جنگ نرم، همان فضای مجازی است.

فضای سایبر، دارای شاخصه ها و ویژگیهایی است که آن را از سایر رسانه ها جدا نموده و به عنوان محور اصلی جنگ نرم قرار داده است که به مهم‌ترین آن‌ها اشاره می‌کنیم:

۱ ـ جهانی و فرامرزی بودن: ویژگی منحصر به فردی که فضای سایبر را از دیگر رسانه ها جدا می سازد، همین بُرد جهانی است. این جهانی بودن با ارسال گسترده ی امواج ماهواره ای از یک نقطه ی خاص به سراسر جهان متفاوت است. علاوه بر محدودیت های خاص امواج ماهواره ای در مناطق مختلف و مشکلات فنی و محیطی آن، برنامه های ماهواره ای در یک نقطه ی مخصوص تولید و سپس انتشار می یابند .در حالی که در محیط مجازی اینترنت، امکان تولید جهانی فراهم است.

۲ ـ ویژگی فوق تصور دیگر در فضای مجازی: امکان ارتباط دو طرفه به صورت سهل و آسان است. به عبارتی در این محیط امکان های خاصی ارتباط سریع و آسان کاربران، سرورها و مدیریت کنندگان را امکان‌پذیر می‌سازد. این ویژگی نیز در انواع دیگر رسانه‌ها با محدودیت‌ها و مشکلات خاصی رو به روست.

۳ ـ جذایت و تنوع، ویژگی دیگر فضای مجازی است: ضمن این که امکان بهره‌برداری از همه‌ی جذابیت‌های خاص رسانه‌ای مانند فیلم، عکس و ... همان طور که ذکر شد مشتری مداری محض در تنوع و جذابیت این محیط تأثیر به سزایی دارد. شاخصه‌های دیگری نیز این محیط را برای بهره‌گیری در عرصه‌ی جنگ نرم مهیا می‌نماید.

۴ ـ مخاطب خاص و تاثیرگذار: همین مسأله باعث شده که اینترنت و فضای مجازی نوعی مرجعیت فکری ـ سیاسی را برای کاربران خود ایجاد نماید. گرچه می‌توان ادعا کرد این امر در جوامعی با فراگیری کاربران، موضوعیت خود را تا حدودی از دست داده است؛ اما حداقل در ایران هم چنان به عنوان یک نقش برای فعالین این عرصه تعریف می‌شود.

۵ ـ مسأله‌ی دیگر امکان عبور و عدم تقید به بخش مهمی از قوانین و محدودیت‌های رایج در سایر رسانه‌ها است: این امر به ویژه در محیط‌های غیر رسمی بیشتر رایج است. به عنوان مثال وبلاگ‌ها با گستردگی میلیونی خود توانسته اند مخاطبانی فراگیر جذب کنند که به طور معمول مقید به قوانین خاصی نیستند و چه بسا وبلاگی با مخاطبانی به مراتب بیشتر از یک وب سایت و خبرگزاری رسمی، با دستی باز همه ی خطوط قرمز یک جامعه را زیر پا بگذارد و بتواند از سد فیلترینگ و محدودیت های فنی هم رها شود. یا می توان به کامنت ها و نظرهای کاربران به عنوان یک بخش جذاب اشاره کرد؛ که می تواند از قواعد و رویه‌های موجود استثنا شود.

نقض کپی رایت در فضای سایبری

نقض کپی رایت در اینترنت زمانی رخ می دهد که یکی از حقوق انحصاری (مادی یا معنوی) پدیدآورنده در جریان ارتباطات اینترنتی مورد تجاوز قرار گیرد. از میان این حقوق می‌توان به حق ممانعت دیگران از تولید مجدد یا کپی کردن یک اثر، نمایش یک اثر به عموم یا توزیع و تکثیر آثار اشاره کرد. اکنون اضافه می‌کنیم که عمده‌ترین موارد نقض کپی رایت از سوی ارائه‌دهندگان خدمات اینترنتی یا رسا ها رخ می‌دهد. رسانه‌ها خدمات دسترسی به اینترنت را در ازای دریافت وجه برای مشتریان انجام می‌دهند. آن‌ها همچنین داده‌های مختلفی را برای استفاده مشتریان خود ذخیره می‌کنند که می‌توان به داده های ذخیره شده بر سرور گروه خبری یا سرور اشاره کرد. مسئولیت رسانه‌ها در قبال فعالیت‌هایی که در برابر مشتریان شان انجام می‌دهند عموما بر آگاهی آن‌ها از فعالیت های مشتری مبتنی است. ارائه‌دهندگان خدمات on-line در صورتی مسئول نقض کپی رایت خواهند بود که به طور مستقیم در کپی کردن یک اثر حمایت شده دخالت داشته باشند. علاوه بر این ارائه‌دهندگان خدمات اینترنتی حتی به طور مستقیم در کپی کردن آثار مورد حمایت دخالت نداشته باشند ممکن است به خاطر نقض کپی رایت مسئول شناخته شوند.(انصاری، ۱۳۸۷).

استفاده منصفانه

حقوق انحصاری پدیدآورندگان آثاری که تحت حمایت قواعد و قوانین کپی رایت هستند با برخی محدودیت‌ها مواجه است. در قوانین بسیاری از کشورها و اسناد بین المللی، یکی از موارد مهم استثنای بر حقوق انحصاری مؤلف استفاده منصفانه» می‌باشد. استفاده منصفانه به استفاده از حق انحصاری دارنده اثر مشمول حمایت در جهت یک هدف متعارف بدون کسب اجازه از دارنده اثر اطلاق می‌شود. هدف از پیش بینی چنین استثنایی را بایستی در اصول بنیادین حقوق بشر ازجمله اصل آزادی بیان جستجو نمود.

استثنای مربوط به استفاده منصفانه از استثنائات کلی بر حقوق مؤلف است و برای منصفانه تلقی شدن استفاده از یک اثر عوامل و مؤلفه‌های متعددی در قوانین مربوط پیش بینی شده است. در نظام حقوقی ما نیز قانون‌گذار در منابع قانونی مربوط به حقوق مؤلف بدون تصریح و ذکر عوامل مؤثر در شناسایی یک استفاده منصفانه از اثر مشمول حمایت به طور پراکنده موارد استثنا را احصا نموده است که در ذیل ذکر می‌کنیم.

الف: استفاده آموزشی و علمی

از آنجایی که اگر توسعه و گسترش امور علمی و آموزشی که از لوازم پیشرفت تمدن و فرهنگ در جوامع بشری است منوط به اجازه پدیدآورندگان این گونه آثار باشد، بعضا به دلیل عدم دسترسی و یا احیاناً عدم رضایت پدیدآورنده، موجد مشکلاتی خواهد شد؛ بنابراین قانون‌گذاران کشورها، استفاده‌های آموزشی و علمی را از قلمرو رضایت و اجازه پدید آورنده خارج ساخته‌اند. مواد ۷، ۸، ۹، ۱۰ قانون حمایت حقوق مؤلفان و مصنفان و هنرمندان و ماده ۵ قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی به شرح زیر به این نوع از استفاده‌ها پرداخته است. ماده ۷ نقل اثرهایی که انتشار یافته است و استناد به آن‌ها به مقاصد ادبی و علمی و فنی و آموزشی و تربیتی و به صورت انتقاد و تقریظ با ذکر مأخذ در حدود متعارف مجاز است». تبصره: ذکر مأخذ در مورد جزوه هایی که برای تدریس در موسسات آموزشی توسط معلمان آن‌ها تهیه و تکثیر می‌شود الزامی نیست مشروط بر اینکه جنبه انتفاعی نداشته باشد. ماده ۸. کتابخانه های عمومی و موسسات جمع آوری نشریات و موسسات علمی و آموزشی که به صورت غیر انتفاعی اداره می شوند می‌توانند طبق آیین نامه ای که به تصویب هیأت وزیران خواهد رسید از اثرهای مورد حمایت این قانون از راه عکس برداری یا طریق مشابه به آن به میزان مورد نیاز و متناسب با فعالیت خود نسخه‌برداری کنند. ماده ۹. وزارت اطلاعات می‌تواند آثاری را که قبل از تصویب این قانون پخش کرده و یا انتشار داده است، پس از تصویب این قانون نیز کماکان مورد استفاده قرار دهد. ماده ۱۰. وزارت آموزش و پرورش می‌تواند کتاب‌های درسی را که قبل از تصویب این قانون به موجب قانون کتاب‌های درسی چاپ و منتشر کرده است کماکان مورد استفاده قرار دهد. بر مضمون ماده ۱۰ بویژه در وضعیت کنونی ایراداتی وارد است: نخست این‌که در بین وزارت خانه‌ها، تنها وزارت آموزش و پرورش به امر آموزش نمی‌پردازد؛ بنابراین لازم بود ماده به کلیه وزارتخانه‌هایی که با کار آموزش سر و کار دارند و کتاب یا جزوه ضروری یا آموزشی منتشر نموده‌اند، اشاره می‌کرد. دوم اینکه کتاب، ابزار منحصر به فرد در امر آموزش نیست و چه بسا نوارهای صوتی تصویری یا اجرای عمومی یک نمایش بتواند به نحو شایسته‌تری این نقش را ایفا کند. در نتیجه مناسب بود در متن ماده از واژهاثر آموزشی استفاده می‌گردید. همچنین ماده ۵ قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی استثنایی بر حقوق مؤلف پیش بینی شده است که مبنای آن‌ها جنبه آموزشی، علمی استفاده از آثار مورد حمایت است. در قانون حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه‌ای، استثنای مربوط به استفاده با اهداف آموزشی و علمی پیش بینی نشده است. در زمینه آثار الکترونیکی با توجه به اینکه بر اساس ماده ۶۲ قانون تجارت الکترونیکی، چنین آثاری مشمول احکام مقرر در قوانین صدرالذکر می شوند، لذا استثنائا ت مربوط به استفاده با هدف آموزشی و علمی در خصوص آثار ادبی و هنری قابل اعمال است، اما به جهت سکوت قانون حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه‌ای، اعمال این استثنا در مورد نرم افزارهای رایانه‌ای قابل اجرا در محیط های اینترنتی محل تردید است. چرا که در قانون تجارت الکترونیکی احکام جدید و مستقلی در مورد حقوق مالکیت فکری آثار در فضای مجازی و محیط الکترونیکی پیش بینی نشده و صرفا احکام قوانین موجود به این‌گونه آثار تسری داده شده‌اند. لذا چون در قانون حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه‌ای استثنای مربوط به استفاده با اهداف آموزشی و علمی ذکر نشده است اعمال این استثنا و معافیت در مورد استفاده‌های آموزشی و علمی از نرم افزارهای رایانه‌ای در فضای مجازی و اینترنت مورد تردید است.(آیتی، ۱۳۷۵).

ب: استفاده شخصی و خصوصی

ماده ۱۱ قانون حمایت حقوق مؤلفان و مصنفان ناظر به این مورد است. نسخه‌برداری از اثرهای مورد حمایت این قانون، مذکور در بند یک از ماده ۲، ضبط برنامه های رادیویی و تلویزیونی فقط در صورتی که برای استفاده شخصی و غیر انتفاعی باشد مجاز است. صدر ماده ۵ قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی مربوط به استفاده‌های آموزشی و تحقیقات علمی و تبصره آن در

ارتباط با استفاده شخصی و خصوصی است. تکثیر و نسخه‌برداری از کتب و نشریات و آثار صوتی موضوع مواد ۲ و ۳ این قانون به منظور استفاده در کارهای مربوط به آموزش یا تحقیقات علمی مجاز خواهد بود، مشروط بر این‌که جنبه انتفاعی نداشته باشد و اجازه نسخه‌برداری از آن‌ها قبلا به تصویب وزارت فرهنگ و هنر رسیده باشد.

تبصره: نسخه‌برداری از کتب و نشریات و آثار صوتی موضوع مواد ۲ و ۳ این قانون در صورتی که برای استفاده شخصی و خصوصی باشد بلامانع است.

شایان ذکر است ماده ۴۱ قانون حق مؤلف فرانسه با مجاز دانستن نمایش های خصوصی و غیر انتفاعی در محافل خانوادگی» مفهومی روشن تر و وسیع تر از کلمه شخصی و خصوصیرا نسبت به قانون ایران به دست داده است...(آیتی، ۱۱۰:۱۳۷۵).

نقض حریم خصوصی در فضای سایبری

انسان به حکم طبیعت و سرشت باید دارای حریم خصوصی برای خود باشد و از آن محافظت نماید. در مقابل افراد نیز بایستی نسبت به صیانت و رعایت حریم خصوصی سایرین اقدام نمایند. نقض حریم خصوصی در فضای سایبری یکی از مهمترین مسائل روز جامعه است که از دو منظر قابل بررسی می باشد. یکی از جانب قربانیان نقض حریم خصوصی در فضای سایبری و دیگری از سوی ناقضین حریم خصوصی در فضای سایبری. نگارنده همواره بر این نکته تاکید دارد که بزه دیدگان در فضای سایبری نقش مهمی در بروز جرایم ناقض حریم خصوصی ایفا می‌کنند و در عین حال می‌توانند در اقدامات پیشگیرانه علیه جرایم سایبری[1]نقش آفرین باشند. بسیاری از بزه دیدگان جرایم سایبری و کسانی که حریم خصوصی آنان در فضای سایبری نقض می‌شود، استعدادی قابل توجه برای قربانی شدن[2]بروز می‌دهند و براحتی طعمه بزهکاران سایبری می‌شوند. برخی کلاهبرداری‌های اینترنتی ناشی از کسب اطلاعات به روش‌های بسیار ساده و سوء استفاده از عکس‌ها و اسرار شخصی نمونه‌هایی از این موضوع می‌باشد. ضعف شخصیتی، فقدان اطلاعات کافی در رابطه با محیط مجازی و عدم دقت در محافظت از داده‌ها و... مواردی است که قربانی بزه سایبری را در قربانی شدنش مساعدت می‌کند. در ابتدای این بحث اعلام گردید که افراد بایستی نسبت به صیانت از حریم خصوصی شان همت نمایند. حال آن که بسیاری از افراد بدون رعایت مسائل امنیتی، خصوصی ترین اطلاعات خود را بر روی سیستم رایانه و یا حامل‌های داده، نظیر فلش و کارت های حافظه و تلفن همراه و سی دی و... ذخیره می‌نمایند که به نوعی دست بزهکار سایبری را در تعرض به حریم خصوصی باز می‌گذارند. به همین خاطر زمینه قربانی شدن در فضای سایبری را بروز می دهند. با الهام از این ضرب‌المثل که (مالت را حفظ کن، همسایه ات را دزد نکن) می‌توان گفت: باید در فضای سایبری از اطلاعات شخصی و حریم خصوصی خود محافظت نماییم تا مجبور نباشیم به دنبال مجرم بگردیم. هرچند این مطلب هیچگاه به معنای توجیه عملکرد بزهکار سایبری نیست یعنی اگر افراد در محافظت از اطلاعات شخصی و یا حریم خصوصی خود کوتاهی نمایند دلیل بر آن نیست که ما خود را مجاز به تعرض به حریم خصوصی افراد بدانیم (طرزی، ۱۳۹۱).

مصادیق نقض حریم خصوصی در فضای سایبری

جنبه دیگر موضوع نیز مربوط به ناقضان حریم خصوصی در فضای سایبری است. این بزهکاران زمانی که وارد فضای سایبری یا همان اینترنت می‌شوند در خیالی خام آن را (ملک طلق) خود دانسته و اجازه هرگونه فعالیت و ورود به حریم خصوصی دیگران را به خود می‌دهند. در ادامه به برخی مصادیق نقض حریم خصوصی در فضای سایبری که در قانون جرایم رایانه‌ای جرم انگاری شده می‌پردازیم:

۱- دسترسی غیرمجاز به داده‌های رایانه‌ای یا مخابراتی نظیر هک ایمیل یا اکانت افراد

1cyber prevention

2mmolate

۲-شنود غیرمجاز محتوای در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی نظیر استفاده از کی لاگرها و نرم افزارهای شنود چت های اینترنتی و...

۳- دسترسی غیرمجاز به داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده یا تحصیل و شنود آن.

۴- در دسترس قرار دادن داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده برای اشخاص فاقد صلاحیت.

۵- نقض تدابیر امنیتی سیستم‌های رایانه‌ای یا مخابراتی به قصد دسترسی به داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده.

۶- حذف یا تخریب یا مختل یا غیرقابل پردازش نمودن داده‌های دیگری از سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده به طور غیرمجاز.

۷- از کار انداختن یا مختل نمودن سیستم‌های رایانه‌ای یا مخابراتی بطور غیرمجاز نظیر غیرفعال سازی دیتابیس تارنماها و ممانعت از دسترسی افراد به سایت‌های شخصی.

۸- ممانعت از دسترسی اشخاص مجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی به طور غیرمجاز.

۹- ربودن داده‌های متعلق به دیگری به طور غیرمجاز.

۱۰- هتک حیثیت از طریق انتشار صوت و فیلم تحریف شده دیگری به وسیله سیستم‌های رایانه‌ای یا مخابراتی.

۱۱- نشر اکاذیب ازطریق سیستم‌های رایانه‌ای یا مخابراتی به قصد اضرار به غیر یا تشویش اذهان عمومی.

۱۲- فروش یا انتشار یا در دسترس قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی متعلق به دیگری را فراهم می‌کند.

۱۳- آموزش نحوه ارتکاب جرایم دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی.

همچنین باید توجه داشت که ناقضین حریم خصوصی در فضای سایبری به دلایلی نظیر افسردگی، عصبانیت، حسادت، انتقام‌جویی، حس تنفر، تفریح و سرگرمی، خودکم بینی و حقارت، حس رقابت و عدم توجه به اصول اخلاقی و ارزش‌های جامعه، خود را مجاز به ورود به حریم خصوصی قربانیان دانسته و خسارات جبران ناپذیری را به حیثیت و مال و حتی جان افراد وارد می‌سازند. (طرزی، ۱۳۹۱).

مسؤولیت‌های ناشی از نقض حریم خصوصی

ضرورت رعایت حریم خصوصی افراد توسط حکومت جمهوری اسلامی ایران با استناد به آیات قرآن ازجمله آیات ۲۷ و ۲۸ سوره نور که اشاره به حریم خصوصی مکانی دارد و همچنین تاکید روایات بر ممنوعیت تجسس در امور دیگران روشن است. امام خمینی که در تمامی عرصه‌ها، خط‌مشی اسلامی داشت حریم خصوصی مردم را پیامبرانه پاسداری کرد ایشان در تاریخ ۶۱/۹/۲۴ فرمان هشت ماده‌ای خطاب به قوه قضاییه و تمام ارگان‌های اجرایی در مورد اسلامی شدن قوانین صادر کرد و در این فرمان ورود بدون اذن به منازل و محل کار افراد و شنود تلفن و گوش دادن به نوار و ضبط‌صوت دیگران به نام کشف جرم و تجسس در اسرار دیگران و افشای آن را ممنوع و جرم دانست.(http://www. islamy-abank. Com)

در اصول ۲۲ و ۲۳ و ۲۵ قانون اساسی جمهوری اسلامی نیز رد پای توجه به این حق را می‌توان پیدا کرد. اصل ۲۲ قانون اساسی می‌گوید:" حیثیت، جان، مال، حقوق و مسکن افراد از تعرض مصون است مگر در مواردی که قانون تجویز کند. "اصل ۲۳ هم تفتیش عقاید را ممنوع کرده و اصل ۲۵ این مسئله را بیان می‌کند که «بازرسی، نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آن‌ها استراق سمع و هرگونه تجسس ممنوع است مگر به‌حکم قانون».(جهانگیر ، ۱۳۸۳). بااین‌همه لزوم تدوین قانون خاص برای رعایت حریم خصوصی احساس می‌شود چراکه قانون اساسی به کلیات می پردازد و جزییات آن بر عهده قانون عادی است تا در آن حدودوثغور این حریم و جنبه‌های مختلف آن و

همچنین تعیین مجازات توجه شود. بااین‌همه طرح حمایت از حریم خصوصی که در تاریخ ۸۵/۴/۸ به چاپ رسید می‌تواند در این زمینه راهگشا باشد. در این طرح به حریم خصوصی جسمانی، منازل، محل کار، حریم خصوصی اطلاعات، اطلاعات شخصی در فعالیت‌های رسانه‌ها، حریم خصوصی ارتباط است و مسئولیت‌های ناشی از نقض حریم خصوصی توجه شده است. یکی از مباحث یاد شده در این طرح که مرتبط با این مقاله است حریم خصوصی و ارتباطات اینترنتی در هفت ماده می‌باشد.

در ماده ۶۵ این طرح آمده «شنود، ضبط، ذخیره یا انواع دیگر رهگیری ارتباطات خصوصی اینترنتی اشخاص بدون رضایت آن‌ها مجاز نیست» ماده ۶۶ نیز بیان می‌کند که ارائه‌دهندگان خدمات عمومی ارتباطات اینترنتی باید کلیه تدابیر فنی و اداری را برای تأمین امنیت و خدمات خود فراهم آورند. و برابر ماده ۷۲ چنانچه درنتیجه نقض حریم خصوصی، خسارت‌های مادی یا معنوی به اشخاص واردشده باشد زیان‌دیده می‌تواند طبق قواعد مسؤولیت مدنی جبران کلیه خسارت‌های خود را مطالبه کند.

هتک حرمت و اشاعه اکاذیب در فضای سایبری از منظر قوانین

فصل پنجم از قانون نوپای جرائم رایانه‌ای به این مهم اختصاص دارد و در طی سه ماده و یک تبصره در شماره‌های ۱۶، ۱۷ و ۱۸ به آن می‌پردازد.

ماده ۱۶ قانون جرائم رایانه‌ای می‌گوید: هر کس به‌وسیله سامانه‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به‌نحوی‌که عرفا موجب هتک حیثیت او شود، به پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد. قابل‌ذکر است که اگر تغییر یا تحریف به‌صورت مستهجن باشد علاوه بر این که به فرد بزه دیده آسیب جدی می‌رسد، نوعی اشاعه فحشا نیز می‌باشد که جرم از زمره جرائم علیه عفت و اخلاق عمومی نیز می‌باشد و نمایش آن طبق بند اول ماده ۶۴۰ قانون مجازات اسلامی عفت و اخلاق عمومی را جریحه‌دار می‌نماید. پس لازم است قانون‌گذار در این مورد شدت عمل بیشتری به خرج دهد. ماده ۱۷ بیان می‌دارد: هر کس به‌وسیله سامانه‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او جز در موارد قانونی منتشر کند یا در دسترس دیگران قرار دهد، به‌نحوی‌که منجر به ضرر یا عرفا موجب هتک حیثیت او شود، به حبس از نودویک روز تا دو سال یا جزای نقدی از پنج میلیون ریال تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد. گویا این ماده تنها اختصاص به هتک حرمت دارد و نشر اکاذیب مقصود نبوده است و انتشار اسرار و مسائل خصوصی خانواده مدنظر قانون‌گذار بوده است تا حریم خصوصی افراد محفوظ بماند. در ماده ۱۸ قانون‌گذار می‌گوید: هر کس به‌قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به‌وسیله سامانه رایانه‌ای یا مخابراتی اکاذیبی را منتشر نماید، یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را برخلاف حقیقت، راسا یا به‌عنوان نقل‌قول، به شخص حقیقی یا حقوقی به‌طور صریح یا تلویحی نسبت دهد، اعم از این‌که از طریق یادشده به نحوی از انحا ضرر مادی یا معنوی به دیگری وارد شود یا نشود، افزون بر اعاده حیثیت (در صورت امکان) به حبس از نودویک روز تا دو سال یا جزای نقدی از پنج میلیون تا چهل میلیون یا هر دو مجازات محکوم خواهد شد.

به نظر می‌رسد ماده ۶۹۸ قانون مجازات اسلامی نیز دقیقه حاوی همین ماده است و مقصود قانون‌گذار تنها منتشر شدن اکاذیب باشد به هر شکل ممکن، و نوع وسیله چندان در جرم دخیل نبوده و شامل اینترنت نیز می‌شود، چراکه انتشار در آن بسیار وسیع‌تر صورت می‌گیرد؛ ایمیل یا پیام‌های متنی تلفنی خود نوعی مراسله به شمار می‌آید؛ پس قانون‌گذار نوع ارسال و انتشار را مدنظر نداشت. کما این‌که روی سایت گذاشتن اکاذیب نیز نوعی رساندن مطلب به دیگران است، چنان چه اگر کسی اکاذیبی را از کسی بنویسد ولی آن را منتشر نسازد مرتکب جرمی نشده است. آیا حذف و توهین و افترا توسط رایانه صورت می‌پذیرد؟

توهین در فضای سایبری

در اصطلاح حقوقی، توهین یا اهانت کاری است که متضمن اسناد و اخبار نبوده و به نحوی از انحا در حیثیت متضرر از این جرم، نوعی وهن وارد می‌کند. افترا متضمن اسناد است و حال‌آنکه توهین غالباً با الفاظ فحش و تحقیر محقق می‌شود و اشاره یا عمل موهن هم قائم‌مقام همین الفاظ می‌باشند. ماده ۶۰۸ قانون مجازات اسلامی دراین‌باره می‌گوید: "توهین به افراد از قبیل

فحاشی و استعمال الفاظ رکیک چنان چه موجب حد قذف نباشد، به مجازات شلاق تا ۷۴ ضربه و پنجاه هزار تا یک میلیون، جزای نقدی محکوم می‌شود ". قانون‌گذار علاوه بر ماده ۶۰۸ قانون مجازات اسلامی با توجه به شخصیت و مقام طرف اهانت، مواد دیگری را تصویب کرده است. ازجمله مواد ۵۱۳، ۵۱۴ و ۶۰۹ قانون مجازات اسلامی، ماده ۲۴ قانون وکالت، ماده بیستم لایحه قانونی استقلال کانون وکلای دادگستری و ماده سی‌ام قانون مطبوعات. شایان‌ذکر است آنچه در اینجا مدنظر است نحوه تحقق اصل جرم توهین می‌باشد؛ یعنی امکان تحقق توهین ساده، با توجه به شرایط آن در اینترنت یا رایانه وجود دارد یا خیر؟ قانون مجازات جرائم رایانه‌ای که شورای عالی توسعه قضایی تدوین کرده، به جرم توهین اشاره نشده است. گرچه همان‌گونه که ذکر شد توهین یکی از مصادیق بارز هتک حرمت و نشر اکاذیب است. چراکه با توهین به کسی حرمت او از بین می‌رود و ازآن‌جهت که نسبت داده‌شده واقعیت ندارد نوعی جرم است و انتشار آن در اینترنت نوعی انتشار اکاذیب است. منطوق صریح ماده ۶۰۸ قانون مجازات اسلامی نفس توهین را مجازات نموده است، و می‌دانیم که توهین به روش‌های مختلفی صورت می‌گیرد که این ادعای ما را مواد قانونی۶۹۷، ۶۹۸، ۶۹۹ و ۷۰۰ قانون مجازات اسلامی تائید می‌کند یکی از این روش‌ها کاربرد اینترنت می‌باشد که امروزه بسیار شایع می‌باشد ماده ۶۹۷ قانون مجازات اسلامی کاملاً مشمول توهین اینترنت می‌شود، چون آمده: ". . . در روزنامه جراید نطق در مجامع یا به هر وسیله دیگر. . . " و قید به هر وسیله دیگر بیانگر این موضوع است که قانون‌گذار می‌خواهد به هر نحوی که شده است، جلوی چنین جرمی را بگیرد و اصل جرم از نظر او دارای اهمیت است که صورت نگیرد و یکی از این راه‌ها اینترنت می‌باشد.

مفاد ماده ۶۹۸ قانون مجازات اسلامی به‌طور صریح علت مجازات را بیان می‌کند و می‌گوید: "هرکسی به‌قصد اضرار به غیر یا تشویش اذهان. . . " این تحلیل گویای این مطلب است که هرگاه این قصد حاصل شود، ملازمه‌اش مجازات مذکور در ماده‌قانونی است، یعنی به‌بیان‌دیگر نوعی تلازم وضعی بین قصد و مجازات وجود دارد، حال هر چیزی این ملازمه را به وجود بیاورد، به‌تبع آن مجازات مذکور باید جاری گردد و می‌توان گفت که از طریق رایانه قصد فوق حاصل می‌گردد؛ یعنی هم اضرار مادی و هم اضرار معنوی حاصل می‌شود و اینترنت به‌عنوان ابزار پیشرفته برای چنین جرائمی محیطی باز محسوب می‌شود. اینترنت می‌تواند یکی از مصادیق ماده ۶۹۹ قانون مجازات اسلامی باشد، چون در آن ذکرشده است: ". . . به نحوی متعلق به او قلمداد نماید. " و قید به نحوی بسیار کلی و جامع است، یعنی قانون‌گذار هر کسی از هر راهی که چنین جرمی را مرتکب گردد، مجازات می کنند و امروزه از طریق اینترنت ارتکاب چنین جرمی ممکن است و صورت گرفته است. اساسا با این قید مذکور ماده فوق مفهومش بر اتهام اینترنتی بار می‌شود و تهمتی اینترنتی یکی از مصادیق آن محسوب می‌شود. ماده ۷۰۰ قانون مجازات اسلامی هم نیز شامل هجو اینترنتی می‌شود از طریق اینترنت یا در اختیار داشتن آدرس‌های الکترونیکی داده هایی را که از هجویات باشند، پست‌نماید و با این عمل فردی را متهم به امور غیر واقع نماید. امروزه شبکه‌اینترنت که هدفش اطلاع‌رسانی است، در دایره مطبوعات وزیر مجموعه جراید بوده و می‌توان گفت که اگر مواد قانونی موجود شامل جراید و روزنامه‌ها باشد، پس شبکه‌اینترنت نیز می‌تواند در دسته جراید قرار گیرد و مشمول احکام آن گردد. پس می‌توان گفت:

الف) توهینی که از طریق اینترنت صورت می پذیرد، جرم است.

ب) هر جرم درخور کیفر و مجازات می‌باشد.

پس توهینی که از طریق اینترنت صورت می پذیرد به خاطر جرم بودن در خور کیفر و مجازات می‌باشد، با توجه به تعریف فقهی که از جرم ارائه شده است، عناصر و شرایطی را که یک جرم دارد، کاملا منطبق این مورد می‌باشد. پس هر کسی (انسان عامل، بالغ، مختار و قاصد) از طریق اینترنت دشنام بدهد، یا عملی را انجام دهد که دیگری را متهم به اموری نماید که شرع ممنوع گردانیده است و صحت و سقم این نسبت ناروا را نتواند ثابت کند، جرم محسوب شده و علاوه بر اعاده حیثیت و جبران ضرر مادی و معنوی به حبس محکوم می‌گردد (مواد ۶۰۸، ۶۰۹، ۶۹۷ و ۶۹۸ قانون مجازات اسلامی) و (ماده ۳۰ قانون مطبوعات سال ۶۴ (ماده یک قانون مسئولیت مدنی).

Email

افترا در فضای سایبری

افترا نیز از مصادیق هتک حرمت است ولی در قانون جرائم رایانه‌ای به آن پرداخته نشده است در حالی که حرمت افترا از امور مسلم فقهی است و روایات متعددی بر آن دلالت می‌کند. (حر عاملی، م بی تا) افترا عین انتساب امری مجرمانه و با انتشار جرم انتسابی به یکی از طرق قانونی و امثال آن. افترا در اصطلاح حقوقی عبارت است از نسبت دادن صریح عمل مجرمانه برخلاف حقیقت و واقع به شخص یا اشخاص معین به یکی از طرق مذکور در قانون، مشروط به این که صحت عمل مجرمانه نسبت داده شده در نظر مراجع و مقامات قضایی ثابت نشودجرم افترا موضوع ماده ۶۹۷ قانون مجازات اسلامی در سال ۱۳۰۴ و در قانون مجازات عمومی به موجب ماده ۲۶۹ وضع گردید که به این شرح است:"هر کس به وسیله اوراق چاپی یا خطی یا به وسیله انتشار اعلام یا اوراق مزبور، یا به وسیله نطق در مجامع به یک یا چند نفر امری را به طور صریح نسبت دهد که مطابق قانون، مجازات آن امر جنحه یا جنایت محسوب شود، مفتری محسوب خواهد شد، مشروط بر این که نتواند صحت آن اسناد را ثابت نماید. "در سال ۱۳۶۲ با تصویب قانون مجازات اسلامی (تعزیرات) این جرم به موجب ماده۱۴۰ جایگزین ماده ۲۶۹ ق. م. ع گردید و در سال ۱۳۷۵ ماده ۶۹۷ ق. م. ا به شرح ذیل بهاین جرم اختصاص یافت. "هر کس به وسیله اوراق چاپی یا خطی یا به وسیله درج در روزنامه و جراید یا نطق در مجامع یا به هر وسیله دیگر به کسی امری را به طور صریح نسبت دهد، یا آن‌ها را منتشر نماید، که مطابق قانون آن امر جرم محسوب شود، و نتواند آن اسناد را اثبات نماید، جز در مواردی که موجب حد است، به یک ماه تا یک سال حبس و تا ۷۴ ضربه شلاق یا یکی از آن‌ها حسب مورد محکوم خواهد شد.

تبصره: در مواردی که نشر آن امر اشاعه فحشا محسوب گردد، هر چند بتواند صحت اسناد را ثابت نماید، مرتکب به مجازات مذکور محکوم خواهد شد

علاوه بر این، افترا به اشخاص حقیقی و حقوقی (اگر چه از طریق انتشار عکس یا کاریکاتور باشد) در اجرای بند هشتم ماده ششم قانون مطبوعات (مصوب ۱۳۶۴. ۱۲. ۲۲ یا اصلاحات ۱۳۷۹. ۹. ۲۲)، به وسیله نشریات منع شده است. در همین خصوص ماده سی ام قانون مطبوعات می گوید:انتشار هر نوع مطلب مشتمل بر تهمت یا افترا یا فحش و الفاظ رکیک یا نسبت های توهین آمیز و نظایر آن نسبت به اشخاص ممنوع است. مدیرمسوول جهت مجازات به محاکم قضایی معرفی می گردد و تعقیب جرائم مزبور موکول به شکایت شاکی خصوصی است و در صورت استرداد شکایت، تعقیب در هر مرحله ای که باشد متوقف خواهد شد.

تبصره یک: در موارد فوق شاکی اعم از حقیقی یا حقوقی می‌تواند برای مطالبه خساراتی که از نشر مطالب مذکور بر او وارد آمده، به دادگاه صالحه شکایت نموده، و دادگاه نیز مکلف است نسبت به آن رسیدگی و حکم متناسب صادر نماید.

تبصره دو: هرگاه انتشار مطالب مذکور در ماده فوق راجع به شخص متوفا بوده، ولی عرفا هتاکی به بازماندگان وی به حساب آید، هر یک از ورثه قانونی می‌تواند از نظر جزایی یا حقوقی طبق ماده و تبصره فوق اقامه دعوی کند.

تبصره سه ماده اول قانون مذکور در این راستا مقرر داشته است: کلیه نشریات الکترونیکی مشمول مواد این قانون است.

بنابراین می‌توان گفت که در مورد افترای درفضای مجازی قانون‌گذار ایران، به طور صریح واکنش نشان داده است، ولی این واکنش، مختص نشریات الکترونیکی است. طبق ماده ۶۹۷ قانون مجازات اسلامی، تحقق جرم افترا مشروط به آن است که مرتکب یکی از راه های مذکور در ماده مذکور را عملی سازد. وسیله اسناد عبارت است از اوراق چاپی یا خطی و انتشار آن‌ها، درج در روزنامه و جراید و نطق در مجامع. حال سوال این است که آیا رایانه و اینترنت می‌تواند وسیله اسناد تحقق این جرم قرار گیرد؟به عبارت دیگر آیا عبارت: به هروسیله دیگر شامل رایانه هم می‌شود ؟مثلا شخص از طریق گفت و گو (چت)، فرستادن ایمیل یا با نقاشی و کاریکاتور طرفمقابلرابهارتکابعملیکهدرقانونجرماست، متهم کند. برخی بدون این که اشاره ای به رایانه و اینترنت داشته باشند، معتقدند که راه های مذکور در ماده ۶۹۷ قانون مجازات اسلامی اصولا به صورت نوشته یا گفتار است و لذا در تسری طرق ارتکاب جرم افترا به موارد دیگر مماثلت و مشابهت باید رعایت گردد. با این تفسیر رایانه و اینترنت شامل ماده ۶۹۷می‌باشد و تفسیر مضیق قوانین کیفری نیز چنیناقتضامی‌کند. اما در این باره نظریات مخالفی هم وجود دارد. در کتاب جرائم علیه اشخاص آمده است این جرم مقید به وسیله است، اما از نظر نوع وسیله، محدودیتی وجود نداردمقنن پس از احصا، بعضی از مصادیق مقرر می دارد: ". . . یا به هر وسیله دیگر. . . ". بنابراین می‌توان با وسایلی مانند رادیو، تلویزیون، سینما، تئاتر، رایانه (اینترنتی) و امثال آن‌ها نیز

مرتکب جرم افترا شد. جمله اخیر نافی شرط وسیله نیست، بلکه نافی محدودیت مصداقی است، زیرا تا سال ۱۳۷۵ که اشکال رفع نشده بود، همواره مشکل شمول ماده بر انتساب جرم از طریق رادیو و تلویزیون مطرح بود. به نظر می رسد که ماده ۶۹۷ قانون مجازات اسلامی اطلاق دارد. ضمنا هدف قانون‌گذار به کار بردن "به هر وسیله دیگر" عمدی بوده تا راه های اسناد افترا را محدود نکند. به عبارت دیگر، هدف مقنن نه این که نوع وسیله را بیان کند. چه تفاوتی می‌کند که شخص از طریق رایانه و انتشار در اینترنت عمل مجرمانه را به دیگری نسبت دهد و یا از طریق یک نوشته که در اولی حتی آثارش مخرب تر از دومی است. بنابراین هر چند جهت رفع ابهامات، نص قانونی خاصی را در این مورد می طلبد، ولی در حال حاضر به نظر می رسد طبق ماده ۶۹۷ ق. م. ا چنین افتراهایی جرم و قابل مجازاتند. گفتنی است که اگر مطالب افتراآمیز در روزنامه‌ها و مجلات الکترونیکی صورت بگیرد، (همانطور که قبلا مطرح شد) اشکالی در جرم دانستن آن‌ها وجود ندارد. به نظر می رسد که جرم افترا توسط رایانه هم صورت می پذیرد، چرا که وقتی نص قانون هست که نوع وسیله را آزاد گذاشته، دیگر جای مخالفتی نمی ماند. از آنجا که تکنولوژی روز به روز در حال ترقی و پیشرفت است و انسان ها برای رسیدن به مقاصد خود از آن بهره می گیرند، پس قانون‌گذار این مساله را در نظر داشته است و ازاستفاده کرده است که در هر عصری بتوان با مجرمان که باعث آزار و اذیت دیگران می شوند و سلب آسایش می کنند، برخورد مناسبی شود و مقید به نوع و وسیله ارتکابی خاص نبود. پست الکترونیک مرسوم ترین و گسترده ترین سرویس شبکه‌های کامپیوتری و بین المللی است و توسط آن علاوه بر فایل های متن، صوت، تصویر، فایل های ویدئویی نیز می‌تواند از طریق پست الکترونیک به دیگر کاربران شبکه (اینترنت) ارسال شود. هر کاربر می‌تواند در شبکه‌های بین المللی از طریق یک آدرس مشخص الکترونیک شناخته شود که با دسترسی به رمز آن می‌توان به آسانی در آن تقلب کرد. این قابلیت پست الکترونیک می‌تواند ابزاری جالب برای نشر اطلاعات مجرمانه یا نشر اکاذیب و افترا به اشخاص باشد و احتمال کنترل اطلاعات برای تهیه کننده کاملا مشکل است و در عمل به خاطر تعداد بسیار زیاد پست الکترونیک ارسالی اتخاذ تدابیر کلی و گسترده امنیتی مشکل بوده و تنها برای بخش کوچکی از داده ها میسر می‌باشد. قذف در رایانه نیز صورت می‌گیرد و آثار مخرب تری دارد. سزاوار است که قانون‌گذار برای حفظ آبروی افراد شدت عمل بیشتری در مورد قذفی که در رایانه صورت می‌گیرد نشان دهد. توهین یکی از مصادیق بارز هتک حرمت و نشر اکاذیب است. چرا که با توهین به کسی حرمت او از بین می رود و از آن جهت که نسبت داده شده واقعیت ندارد نوعی جرم است و انتشار آن در اینترنت نوعی انتشار اکاذیب است. افترا نیز مصداق دیگر هتک حرمت است. افترا مقید به وسیله است، اما از نظر نوع وسیله، محدودیتی وجود ندارد. مقنن پس از احصاء بعضی از مصادیق مقرر می دارد: ". . . یا به هر وسیله دیگر. . . " بنابراین می‌توان با وسایلی مانند رادیو، تلویزیون، سینما، تئاتر، رایانه (اینترنتی) و امثال آن‌ها نیز مرتکب جرم افترا شد (دزیانی، ۸۰).

مسئولیت مدنی ناشی از هتک حرمت درفضای سایبری

هر ضرری اعم از مادی و معنوی به اشخاص باید جبران شوداگر شخصی مورد نشر اکاذیب یا افترا یا هتک حیثیت واقع شود، به نوعی متحمل ضرر و زیان معنوی شده است و علاوه بر اینکه می‌تواند عامل این ضرر رسانی را از طریق مراجع قضایی به مجازات برساند، بلکه بر اساس اصول حقوقی حق دارد خسارات ناشی از این ضرر و زیان معنوی را نیز مطالبه کند. در همین راستا در ماده ۱ قانون مسئولیت مدنی آمده است هر کس بدون مجوز قانونی به حیثیت سایرین لطمه‌ای وارد کند که موجب ضرر و زیان مادی یا معنوی شود، مسئول جبران خسارات ناشی از عمل خویش است. جدا از ماده ۱ قانون مسئولیت مدنی، در مواد ۲ و ۹ و ۱۰ این قانون نیز به عناوین گوناگون از خسارات معنوی یاد شده است. در رویه قضایی ما موارد عملی زیادی در این خصوص قابل مشاهده نبوده و نیست. از این‌رو به نظر می‌رسد قوانین جزایی ایران در این باب با نواقصی همراه است. اگر چه در قانون مطبوعات تلاش شده است تا حدی این نواقص بر طرف شود. به عنوان مثال بر اساس قانون مطبوعات اگر در روزنامه‌ای در خصوص شخصی مطلبی حاوی هتک حیثیت درج شود، آن روزنامه موظف است در شماره بعدی خود، در همان صفحه و همان ستون، جوابیه آن مطلب را نیز درج کند. البته این مقدار، از دید بسیاری از حقوقدانان کافی نبوده و نیست. چراکه وقتی آبروی شخصی در افکار عمومی یا حتی در یک جمع خاص از دست برود، احیای آن با انتشار یک جوابیه صورت نخواهد گرفت.

مسئولیت مدنی ناشی از نفوذ و هک سیستم

یکی از بخش‌های مهم و اصلی در ارتکاب جرائم سایبری مربوط به بخش سرقت اطلاعات «هک و نفوذ» است. هکرها با استفاده از ابزارهای متفاوت که به برخی از آن‌ها اشاره خواهیم کرد به اطلاعات شخصی و محرمانه افراد دست می‌یابند. اطلاعاتی که مربوط به حریم خصوصی و شخصی افراد می‌باشد و مسلماً به هیچ وجه راضی به افشا و دسترسی به آن، توسط افراد غریبه نیستند، این اطلاعات می‌تواند شامل: رمزهای عبور، عکس‌های خانوادگی، اطلاعات بانکی، مشخصات و اطلاعات فردی و بسیاری موارد دیگر باشد؛ اما مسئلهٔ اصلی فقط دست‌یابی به اطلاعات شخصی نیست، بحث اصلی و مهم سوء استفاده‌هایی است که سارقان هویت «هکرها» با استفاده از آن می‌توانند، انجام دهند. سرقت هویت استفاده از هویت شخص دیگر «اطلاعات حساس یا شخصی» برای سوء استفاده مالی و یا سایر اهداف مخرب است. روش‌هایی که در این بخش ذکر خواهیم کرد ازجمله روش‌هایی است که سارقان هویت «هکرها» از آن‌ها استفاده می‌کنند. هکرها به کمک این اطلاعات می‌توانند، ضررهای مادی و معنوی بسیار زیادی را به افراد جامعه وارد کنند و آن‌ها را در معرض خطرهای بی شماری قرار دهند. با توجه به پیشرفت‌هایی که در دنیای کامپیوتر و اینترنت صورت گرفته است زندگی روزمرهٔ ما نیز دست خوش تغییرات فراوانی گردیده است که در بسیاری از موارد این تغییرات مثبت بوده است؛ اما در مواردی هم شاهد اثرات منفی تکنولوژی جدید بر روی روند زندگی خود بوده‌ایم. افراد کلاهبردار و شیاد هم در کنار سایر افراد، از کامپیوتر و اینترنت بهره‌های سود جویانه زیادی می‌برند و در رسیدن به اهداف شوم خود از آن استفاده می‌کنند. به طور کلی هک و نفوذ را هکرها انجام می‌دهند. هکر[1] به معنای نفوذ گر است و به شخصی که هدف اصلی او نشان دادن قدرت خود به کامپیوتر و سایر ماشین‌هاست گفته می‌شود. وارد شدن به سیستم و شکست محاسبات و کنجکاوی در اطلاعات محرمانه ازجمله خصوصیات هکرها است. امروزه هکرها را به چند گروه کلی تقسیم می‌کنند که در ذیل در مورد آن‌ها توضیح خواهیم داد:

گروه نفوذ گران کلاه سفید[2]

این گروه از هکرها در واقع همان دانشجویان و اساتید و دانش آموزان هستند که تنها هدفشان نشان دادن ضعف سیستم‌های امنیتی شبکه کامپیوتر است. این گروه را با عنوان هکرهای خوب نیز می‌شناسند این گروه از هکرها نه تنها مضر نیستند؛ بلکه در تحکیم دیواره حفاظتی شبکه‌ها نقش اصلی و اساسی دارند.

گروه نفوذ گران کلاه صورتی[3]

نام دیگر این گروه است، بوترها افرادی هستند که دارای هیچ گونه توانایی خاصی نیستند و تنها قادر به ایجاد اخلال در سیستم‌ها می‌باشند، کلاه صورتی‌ها اغلب جوانان بی کار و جسوری هستند از نرم افزارهای دیگران استفاده می‌کنند و خود هیچ سوادی در رابطه با برنامه نویسی ندارند.

گروه نفوذ گران کلاه خاکستری[4]

این گروه را با نام واکر می‌شناسند. هدف اصلی این گروه استفاده از اطلاعات سایر کامپیوترها به مقاصد مختلف است، آن‌ها صدمه‌ای را به کامپیوتر وارد نمی‌کنند. این گروه کدهای ورود به سیستم‌های امنیتی را پیدا و به داخل آن نفوذ خواهند کرد؛ اما سرقت و خرابکاری جز کارهای کلاه خاکستری‌ها «واکرها» نیست، بلکه اطلاعات را در اختیار عموم مردم قرار می‌دهند مانند همان کاری که بنیان گذار سایت و یکی لیکس انجام می‌داد و اطلاعات مهم و حساسی را که بعضی از آن‌ها را از این طریق به دست آورده بود به صورت رایگان روی سایت خود قرار می‌داد، البته این مورد نقص قانون جرائم علیه محرمانگی داده‌هاست و مصداق قانونی دارد.

1-Hacker
2-white hat hackers
3- pink hat hackers
4- gray hat hackers

گروه نفوذ گران کلاه سیاه[1]

نام اصلی این گروه کراکر است. کراکرها خرابکارترین نوع هکرها هستند. این گروه به طور کاملاً پنهانی دست به عملیات خراب کارانه می‌زنند. کلاه سیاه‌ها اولین چیزی که به فکرشان خواهد رسید نفوذ به سیستم قربانی است آن‌ها با نفوذ به سیستم قربانی قصد دارند تا به اطلاعات شخصی و هویتی افراد دست یابند، آن‌ها برای این منظور از روش‌های متفاوتی استفاده می‌کنند.[2]

اهداف هکرها

منبع اصلی هکرها به جز هوش سرشارشان، کدهای کامپیوتری است. از آنجایی که اجتماعات بزرگی از هکرها بر روی اینترنت وجود دارند، تنها تعداد اندکی از هکرها شخصاً اقدام به برنامه نویسی می کنند. بسیاری از هکرها به دنبال کدهایی می گردند که دیگران نوشته اند و آن‌ها را از طریق اینترنت دریافت می کنند. در واقع هزاران کد متفاوت وجود دارد که هکرها از طریق آن‌ها به سیستمهای کامپیوتری و شبکه ها نفوذ پیدا می کنند. این برنامه ها به هکرها قدرت زیادی در برابر کاربران و شرکتهای بیگناه می دهند زیرا به مجرد اینکه یک هکر ماهر به طرز کار سیستمی پی ببرد، می‌تواند برنامه ای برای سوءاستفاده از آن طراحی کند. هکرهای بدخواه از برنامه های مذکور برای اهداف زیر استفاده می کنند:

سرقت رمزعبور

راه‌های بسیاری برای هک رمزعبور افراد وجود دارد از حدس‌های مطالعه شده گرفته تا الگوریتم‌های ساده ای که ترکیبات متفاوتی از حروف، اعداد و سمبل ها را تولید می کنند. روش آزمون و خطا در پیدا کردن رمز عبور را حملهBrute force می نامند که در آن هکر سعی می‌کند تمام ترکیبات مختلف را تا پیدا کردن رمز عبور امتحان کند. یک راه دیگر برای هک کردن رمز عبور روش حمله دیکشنری است که در آن یک برنامه کامپیوتری کلمات رایج دیکشنری را در فیلد رمز عبور امتحان می‌کند.

ویروس نویسی

آلوده سازی یک کامپیوتر یا سیستم با ویروس‌ها یکی دیگر از اهداف هکرهای خرابکار است. و یروس‌های کامپیوتری برنامه‌هایی هستند که برای تکثیر خویش برنامه ریزی شده‌اند و منجر به مشکلات مختلفی از قبیل از کار افتادن یک کامپیوتر تا پاک کردن اطلاعات موجود بر روی دیسک سخت می‌شوند. ممکن است هکر با نفوذ به یک سیستم، ویروسی را بر روی آن نصب کند ولی روش رایج بیشتر آن‌ها ایجاد یک ویروس ساده و ارسال آن از طریق ایمیل، پیامهای فوری و یا قرار دادن بر روی وب سایتهای حاوی اطلاعات قابل دریافت وشبکه‌های نظیر به نظیر(P۲P) است (http://fa. wikipedia .org/wiki/ ۱۳۹۲/۳/۳).

دسترسی مخفیانه

مشابه سرقت رمز عبور، برخی از هکرها برنامه هایی را ایجاد می کنند که به دنبال راههای محافظت نشده برای نفوذ به سیستمها و شبکه ها می گردند. در روزهای اولیه اینترنت، بسیاری از سیستمهای کامپیوتری امنیت چندانی نداشته و هکرها می‌توانستند بدون داشتن نام کاربری و رمز عبور راهی را برای نفوذ به سیستم پیدا کنند. یکی از راههای پیدا کردن دسترسی مخفیانه به سیستم، قرار دادن یک تروجان بر روی سیستم قربانی توسط هکر است.۳

ایجاد زامبی

کامپیوتری که تبدیل به زامبی شده است به نام Bot یا ربات نیز شناخته می‌شود و در واقع کامپیوتری است که هکر می‌تواند با استفاده از آن به ارسال هرزنامه بپردازد و یا حملات انکار سرویس توزیع شده را به انجام برساند. بعد از اجرای یک کد به ظاهر بی خطر توسط قربانی، یک راه ارتباطی بین سیستم وی و هکر برقرار می‌شود. بعد از آن هکر می‌تواند به صورت مخفیانه کنترل رایانه قربانی را در دست گرفته و از طریق آن دست به اعمال خرابکارانه و ارسال هرزنامه بزند.۴

جاسوسی ایمیل

---

1 - Black hat hackers

2 - http://news. police. ir/fullStory. do?Id=221591 1392/4/26

3- http://www. certcc. ir

۴ http://fa. wikipedia. org/wiki/۱۳۹۲/۳/۳

هکرها برنامه هایی را ایجاد کرده اند که به آن‌ها اجازه می دهد که ایمیلها را مشاهده کنند یا در واقع به همان استراق سمع رایج بپردازند. امروزه بسیاری از برنامه های ایمیل از شیوه های رمزنگاری پیچیده استفاده می کنند که حتی در صورت لو رفتن ایمیل‌ها، هکرها نتوانند از آن سر در بیاورند.

قانون:گر چه در قوانین کشور ما به جبران خسارت قربانیان ویروس‌های اینترنتی اشاره‌ای نشده است اما مواد قانون مدنی، قانون مسئولیت مدنی و نیز قانون مجازات اسلامی به ما کمک می‌کنند که حکم موضوع را استخراج کنیم (بشری راد و حبیبی، ۱۳۹۱).

اتلاف با تسبیب مال غیر

ماده ۳۲۸ قانون مدنی تلف اموال دیگران را ممنوع و موجب مسئولیت دانسته است «هر کس مال غیر را تلف کند ضامن است و باید مثل یا قیمت آن را بدهد و اگر آن را ناقص یا معیوب کند ضامن نقص قیمت آن مال است». با توجه به این ماده، در ابتدا باید از خود پرسید که آیا اطلاعات در زمره اموال محسوب می‌شوند تا اقدام هکرها به از بین بردن آن‌ها اتلاف به شمار آید یا نه؟در پاسخ باید گفت که اصطلاح مال مفهوم وسیعی دارد و شامل اعیان، منافع، حقوق عدم‌النفع و نیز برخی بخت‌ها و فرصت‌های مسلم مالی می‌شود. حقوق، خود به انواعی تقسیم می‌شود و شامل حق فرد بر تمامیت جسمی، یا بر حیثیت خانوادگی یا بر شهرت تجاری یا آزادی افراد و سایر حقوق مرتبط می‌شود که اتلاف در مورد همه حقوق صرف‌نظر از موضوع آن‌ها ممکن است رخ دهد. منتها سوال این است که آیا ویروسی که یک هکر در شبکه‌اینترنت وارد کرده و از این طریق به اطلاعات و داده‌های نرم‌افزاری افراد صدمه می‌زند وسیله و ابزاری تلقی می‌شود که در دست هکر قرار گرفته است و در نتیجه هکر مباشر به شمار می‌رود یا اینکه ویروس، واسطه میان هکر و خسارات وارد آمده می‌باشد و در نتیجه هکر مسبب به شمار می‌رود و نه مباشر؟در این صورت به ماده ۳۳۱ قانون مدنی می‌توان استناد کرد که مقرر می‌دارد:تفاوت میان اتلاف و تسبیب از این جهت مهم است که در اتلاف تقصیر شرط ایجاد مسئولیت نیست اما در تسبیب عمل مسبب باید تقصیرکارانه باشد. همچنین در اتلاف، شخص مستقیما مال دیگری را تلف می‌کند در حالی که در تسبیب برای اتلاف مقدمه‌سازی می‌شود که احتمال دارد آن مقدمه به نتیجه منجر شود یا این‌که عقیم بماند (کاتوزیان، ۱۳۷۸).

مسئولیت هکرها بر اساس قانون مسئولیت مدنی

ماده یک قانون مسئولیت مدنی مقرر می‌دارد:«هر کس بدون مجوز قانونی، عمدا یا در نتیجه بی‌احتیاطی، به جان یا سلامتی یا مال یا آزادی یا حیثیت یا شهرت جهانی یا هر حق دیگری که به موجب قانون برای افراد ایجاد شده لطمه‌ای وارد کند که موجب ضرر مادی یا معنوی دیگری شود مسئول جبران خسارت ناشی از عمل خود است ». در مورد فعالیت هکرها با توجه به این ماده می‌توان گفت که اگر نتوان اقدام آن‌ها را در حذف، از بین بردن تحریف و بر هم ریختن اطلاعات و داده‌های سیستم‌های رایانه‌ای دیگر تلف مال و مشمول حکم ماده ۳۲۸ قانون مدنی به شمار آورد؛ می‌توان با استناد به این قانون، اقدامات هکرها را تحت عنوان لطمه به مال، حیثیت یا شهرت تجاری یا سایر حقوقی که به موجب قانون برای اشخاص ایجاد شده به شمار آورد و حکم به مسئولت هکرها داد. تفاوتی که مسئولیت مستند بر ماده مذکور با ماده ۳۲۸ قانون مدنی دارد در مبنای مسئولیت هکر است. مسئولیت هکر طبق ماده یک قانون مسئولیت مدنی مبتنی بر تقصیر است در حالی که در ماده ۳۲۸، مسئولیتی است بدون تقصیر.

گریز از فیلترها

فیشرها برای جلوگیری از شناسایی متن‌های متداول فیشینگ در ایمیل توسط فیلترهای ضد–فیشینگ از عکس به جای نوشته استفاده می‌کنند.

جعل وبسایت

برخی از فیشرها از جاوااسکریپت برای تغییر آدرس در نوار آدرس مرورگر استفاده می‌کنند تا هیچ جای شکی برای قربانی نماند. یک مهاجم حتی می‌تواند از ایرادهای موجود در اسکریپت‌های یک سایت معتبر نیز علیه خودش استفاده کند. به این نوع حمله cross-site scripting گفته می‌شود. در این مورد از کاربر خواسته می‌شود تا در بانک خودش لاگین کند. ظاهراً همه چیز عادی است. از آدرس وب‌گاه گرفته تا گواهینامه امنیتی (security certificates). اما در واقعیت، پیوند به آن وب‌گاه دستکاری می‌شود تا

با استفاده از عیب‌های موجود در اسکریپت‌های آن وب‌گاه، حمله انجام شود. با این حال این روش نیازمند دانش و آگاهی بالایی است. از این روش در سال ۲۰۰۶ برای حمله به وب‌گاه PayPal استفاده شد.

فیشینگ تلفنی: تمام حملات فیشینگ نیازمند وبسایت قلابی نیست. پیامهایی که ظاهراً از طرف بانک فرستاده شده و از کاربر می‌خواهد تا مثلاً به دلیل وجود ایراد در حسابشان، شماره خاصی را شماره گیری کنند، نیز می‌تواند حمله فیشینگ باشد. بعد از گرفتن شماره (که متعلق به فیشر است و با سرویس صدا از طریق آی پی مهیا شده‌است)، از کاربر خواسته می‌شود تا شماره حساب و پین(PIN) خود را وارد کند. (مجرب، ۱۳۸۸).

تمرکز برروی کاربر خاص: یکی از راه های فیشینگ تمرکز بر روی کاربر خاص یا یک حوزه خاص در یک تشکیلات است نامه ارسالی ظاهرا خالی از هر گونه اشکال است و انگار از سوی سازمان یا بانک خاصی برای پاسخگویی به یک سوال ارسال شده است. (www. cyberpolice. ir/information/3881)

در حالی که مهمترین هدف آن سرقت اطلاعات شماست. به این ترتیب هکر ها وارد حریم اطلاعات شما می شوند.

مسئولیت مدنی فیشرها

در حال حاضر کاستی‌هایی در ارتباط با قوانین ضد فیشینگ وجود دارد ولی در مجموع با توجه به قانون جرائم اینترنتی و قوانینی که حول و حوش این قانون می‌توان از آن‌ها استفاده کرد و خسارت‌های ناشی از آن را همانند مسئولیت مدنی هکر دانست می‌توان با استناد قانون مسئولیت مدنی، اقدامات فیشرها را تحت عنوان لطمه به مال، حیثیت یا شهرت تجاری یا سایر حقوقی که به موجب قانون برای اشخاص ایجاد شده به شمار آورد و حکم به مسئولیت آن‌ها داد مسئولیت مدنی فیشر طبق ماده یک قانون مسئولیت مدنی مبتنی قابل اثباط بوده وبا توجه به اینکه عمده اهداف یک فیشر دسترسی به اطلاعات و کلیدواژه‌های حساب‌های بانکی و یا اطلاعات خصوصی و محرمانه اشخاص می‌باشد که در پی بدست آوردن آن لطمات مالی و حیثیتی برای افراد متصور است وجود ضرر محرز و در این گونه موارد که نقض حقوق به نحو مستقیم صورت می‌گیرد، مسئولیت شخصی ناقض حقوق مزبور مطلق می‌باشد و اثبات و احراز تقصیر خوانده ضرورت نداشته بلکه صرف اثبات زیان وارده و رابطه سببیت زیان و فعل خوانده کافی است. حتی خوانده نمی‌تواند با اثبات عدم تقصیر خود از مسئولیت فرار نماید.

منابع

۱. انصاری، باقر. (۱۳۸۷). حقوق ارتباط جمعی (چاپ دوم). تهران: انتشارات سمت.

۲. انصاری، باقر، و سایرین. (۱۳۸۱). مسئولیت مدنی رسانه‌های همگانی. تدوین و تنقیح قوانین و مقررات. تهران: انتشارات معاونت پژوهش.

۳. آیتی، حمید. (۱۳۷۵). حقوق آفرینش های فکری با تأکید بر حقوق آفرینش های ادبی و هنری. تهران: نشر حقوقدان.

۴. آیین‌نامه نصب و ثبت اجباری علائم صنعتی، مصوب ۱۳۲۸/۲/۳.

۵. بشری راد، بابک و حبیبی، آرش. (۱۳۹۱). ویروس‌ها و بدافزارهای کامپیوتری. تهران: انتشارات ناقوس.

۶. پاکزاد، بتول. (۱۳۷۵). جرائم کامپیوتری. پایان‌نامه کارشناسی ارشد دانشکده حقوق دانشگاه شهید بهشتی.

۷. پیتر کری، جوساندرز. (۱۳۸۶). حقوق رسانه. ترجمه حمید رضا ملک محمدی. تهران: نشر میزان.

۸. دزیانی، محمد حسن. (۱۳۷۶). نشریه بین‌المللی سیاست جنایی سازمان ملل، شماره‌ها ۳۳ و ۳۴، جزوه جرائم کامپیوتری، جلد ۱، شورای عالی اطلاعات.

۹. فقیه حبیبی، علی و صفایی فر، عباس. (۱۳۹۱). توسعه مسئولیت مدنی در جرائم رسانه‌ها و مطبوعات. فصلنامه علوم خبری، ۹، ۴۱-۲۲.

۱۰. قانون آیین دادرسی دادگاه‌های عمومی و انقلاب (در امور کیفری).

۱۱. قانون تجارت الکترونیکی – مصوب ۱۳۸۲.

۱۲. قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی مصوب ۱۳۵۲.
۱۳. قانون ثبت علائم و اختراعات مصوب ۱۳۱۰/۴/۱ و آیین‌نامه اصلاحی اجرای قانون ثبت علائم تجارتی و اختراعات مصوب ۱۳۳۷.
۱۴. قانون جرائم رایانه‌ای مصوب ۱۱ بهمن ۱۳۸۹.
۱۵. قانون حمایت از حقوق مؤلفان، مصنفان و هنرمندان مصوب ۱۳۴۸.
۱۶. قانون مطبوعات مصوب ۱۳۵۸.
۱۷. قانون مطبوعات مصوب ۱۳۶۴.
۱۸. کاتوزیان، ناصر. (۱۳۷۸). الزام‌های خارج از قرارداد: جلد دوم، مسئولیت مدنی. تهران: انتشارات دانشگاه تهران.