Journal of
International Criminal Law
www.iclj.ir

Volume 4, Issue 1, 2026

Criminal and Civil liability and Damages Caused by Non-Secure Wi-Fi Networks in the Laws of Iran, Germany and the United States

Rohollah Raisizadeh[1], Majid Sarbazian*[2], Dariush Babaei[3]

1. Department of Private Law, Yasouj Branch, Islamic Azad University, Yasouj, Iran.
2. Department of Law, Faculty of Theology and Islamic Studies, Maybod University, Maybod, Iran. (Corresponding Author)
3. Department of Law, Yasouj Branch, Islamic Azad University, Yasouj, Iran.

ARTICLE INFORMATION

Type of Article:
Original Research
Pages: ***31-47***

Corresponding Author's Info
ORCID: *0000-0000-0000-0000*
TELL: *+989177105221*
Email: *hes.6967@gmail.com*

Article history:
Received: *28 Jul 2025*
Revised: *05 Oct 2025*
Accepted: *01 Dec 2025*
Published online: *21 Mar 2026*

Keywords:
Wi-Fi Network, Wireless Network, Civil Liability, Fault, Unsecure Network, Criminal Liability.

ABSTRACT

The expansion of the internet globally has been extensive, and Wi-Fi networks are now an integral part of daily life and business operations. Despite this, Wi-Fi networks, when not secured by their owners (and not the internet service providers), can provide a platform for misuse, harm and Commission of crimes against others. The lack of security in Wi-Fi networks often stems from various reasons, such as the need for open internet access and the convenience of providing services to customers. However, despite numerous warnings, a large portion of Wi-Fi networks remain insecure in various countries. Today, the development of legal systems, including the German legal system, increasingly inclines toward imposing responsibility not only on the direct perpetrator but also on the owner of an insecure Wi-Fi network. This liability is intended to deter the misuse of these networks for harmful activities. This article analyzes and evaluates the approaches of Germany and the United States to this issue and, in the context of Iranian law, proposes that, given the high incidence of crimes committed via insecure Wi-Fi networks, it would be feasible to apply civil liability rules to these network owners under general civil liability principles. Such a measure could serve as an enhanced deterrent, aligning with the secondary objectives of civil liability rules. Moreover, financial penalties might also be imposed on owners of unsecured Wi-Fi networks as a situational crime prevention strategy to curb cybercrimes.

How to Cite This Article: Raisizadeh, R; Sarbazian, M & Babaei, D (2026). "Criminal and Civil liability and Damages Caused by Non-Secure Wi-Fi Networks in the Laws of Iran, Germany and the United States". *Journal of International Criminal Law*, 4(1): 31-47.

فصلنامه حقوق جزای بین‌الملل

www.iclj.ir

انجمن علمی فقه جزای تطبیقی ایران

دوره چهارم، شماره اول، بهار ۱۴۰۵

مسؤولیت کیفری و مدنی و خسارت‌های ناشی از شبکه‌های وای‌فای غیرایمن در حقوق ایران، آلمان و ایالات متحده

روح‌الله رئیسی‌زاده[۱]، مجید سربازیان[*۲]، داریوش بابایی[۳]

۱. دانشجوی دکتری، گروه حقوق خصوصی، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران.

۲. دانشیار، گروه حقوق، دانشکده الهیات و معارف اسلامی، دانشگاه میبد، میبد، ایران. (نویسنده مسؤول)

۳. استادیار، گروه حقوق خصوصی، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۳۱-۴۷

اطلاعات نویسنده مسؤول

کد ارکید: ۰۰۰۰-۰۰۰۰-۰۰۰۰-۰۰۰۰

تلفن: ۰۹۸۹۱۷۷۱۰۵۲۲۱+

ایمیل: hes.6967@gmail.com

سابقه مقاله:

تاریخ دریافت: ۱۴۰۴/۰۵/۰۶

تاریخ ویرایش: ۱۴۰۴/۰۷/۱۳

تاریخ پذیرش: ۱۴۰۴/۰۹/۱۰

تاریخ انتشار: ۱۴۰۵/۰۱/۰۱

واژگان کلیدی:

شبکه وای‌فای، شبکه بی‌سیم، شبکه ناامن، مسؤولیت مدنی، تقصیر، مسؤولیت کیفری.

چکیده

توسعه شبکه اینترنت در سطح جهان بسیار گسترده بوده و امروزه شبکه‌های وای‌فای جزء جدایی‌ناپذیر زندگی و مشاغل است. باوجود این، شبکه‌های وای‌فای (و نه ارائه‌دهنده خدمات رایانه‌ای) که دارنده آن اقدام به تأمین امنیت مناسب آن ننموده، بستر مناسبی برای سوءاستفاده، ایراد خسارت به دیگران و ارتکاب جرایم است. ناامن‌بودن شبکه‌های وای‌فای به‌علل مختلف، همچون لزوم دسترسی آزاد به اینترنت و تسهیل ارائه خدمات به مشتریان صورت می‌گیرد و باوجود تمامی هشدارها، بخش زیادی از شبکه‌های وای‌فای در کشورهای مختلف همچنان ناامن هستند. امروزه تحولات نظام‌های حقوقی، ازجمله نظام حقوقی آلمان، به این‌سو متمایل است که علاوه‌بر شخص مرتکب، بردارنده شبکه وای‌فای ناامن نیز مسؤولیت مدنی و کیفری بار شود که برقراری چنین مسؤولیتی به‌طور مستقیم موجب بازدارندگی از سوءاستفاده از این شبکه‌ها به‌منظور ارتکاب اعمال زیان‌بار خواهد شد. در این مقاله پس از تحلیل و ارزیابی راهکارهای کشورهای آلمان و آمریکا در مواجهه با این مسأله در حقوق ایران، پیشنهاد داده شده است که باتوجه به آمار بالای جرایم صورت‌گرفته از طریق شبکه‌های وای‌فای ناامن، اعمال قواعد مسؤولیت مدنی بر دارندگان این شبکه‌ها بر طبق قواعد عام مسؤولیت مدنی امکان‌پذیر بوده و موجب بازدارندگی بهتر به‌عنوان هدف ثانویه قواعد مسؤولیت مدنی می‌شود. علاوه‌بر این، جریمه مالی نیز می‌تواند در راستای پیشگیری وضعی از جرایم سایبری بر دارندگان شبکه‌های وای‌فای ناامن بار شود.

مقدمه

توسعه استفاده از اینترنت، موجب افزایش موارد اضرار به غیر با استفاده از شبکه اینترنت شده است. این مسأله موجب گردیده تا به موازات بحث جبران خسارت در مسؤولیت مدنی، به هدف ثانویه مسؤولیت مدنی قهری، یعنی بازدارندگی در حوزه اینترنت توجه ویژه‌ای شود، چراکه اقدامات پیشگیری‌کننده معمولاً با صرف وقت و هزینه بسیار کم صورت می‌گیرد، درحالی‌که در کنار آثار وقوع خسارت‌های مالی برای زیان‌دیده، رسیدگی و صدور رأی در این موارد نیز هزینه‌های فراوانی را بر جامعه بار می‌کند. در این موارد بهتر است تا با حذف امکاناتی که انجام اقدامات خلاف قانون را تسهیل می‌کنند، از هزینه‌های فوق پیشگیری نمود و کارآیی قواعد مسؤولیت مدنی را افزایش داد.

در زمینه شبکه‌های وای‌فای محلی ناامن، تحقیقات نشان داده است که وجود این شبکه‌ها یکی از علل افزایش اقدامات خلاف قانون در اکثر کشورها است. همین مسأله موجب توجه حقوق‌دانان و دادگاه به وضعیت این شبکه‌ها و ارائه راهکار در این زمینه شده است. در این خصوص می‌توان ناامن نگه‌داشتن شبکه وای‌فای را جرم‌انگاری نمود و یا با وضع مسؤولیت مدنی، از ناامن باقی‌ماندن شبکه‌های مزبور پیشگیری نمود. در مقاله پیش رو فرضیه اصلی بر این مبنا استوار است که اعمال مسؤولت مدنی (مبتنی‌بر تقصیر یا بدون تقصیر) بر اداره‌کنندگان این شبکه‌ها می‌تواند بر کاهش این اقدامات مؤثر باشد، اما باتوجه به پسینی‌بودن مسؤولیت مدنی بر وقوع عمل خسارت بار و همچنین شدت و وسعت جرایمی که در بستر یک شبکه وای‌فای ناامن اتفاق می‌افتد نیز به حدی است که جرم‌انگاری در قالب جریمه مالی را توجیه می‌کند. در مقابل، برخی معتقد هستند که چنین رویه‌ای در تعارض با حق دسترسی آزاد به اینترنت است که به‌موجب آن، تحدید دسترسی افراد به اینترنت به هر نحوی ممنوع است، لذا به‌منظور بررسی نظریه‌ای که با تأکید بر حق دسترسی آزاد به اینترنت، با اعمال مسؤولیت بر دارندگان این شبکه‌ها مخالف است، موضع حقوق ایالات متحده آمریکا مورد بررسی قرار خواهد گرفت و قواعد عام کامن‌لا در مورد مسؤولیت مدنی دارندگان این‌گونه شبکه‌ها و سپس موضع دیوان عالی آلمان در وضع مسؤولیت بر دارندگان شبکه‌های وای‌فای ناامن که موضعی پیشرو در این زمینه است، مورد نقد قرار خواهد گرفت و درنهایت نیز وضعیت در حقوق ایران مورد نقد و بررسی قرار خواهد گرفت.

۱- تعاریف

در این قسمت به بررسی تعریف شبکه‌های وای‌فای و تفاوت آن با ارائه‌کنندگان خدمات رایانه‌ای خواهیم پرداخت.

۱-۱- شبکه وای‌فای محلی و فراهم آورندگان خدمات رایانه‌ای (رسا)

یک شبکه وای‌فای محلی، شبکه‌ای است که در محیطی کوچک، مانند یک مجتمع مسکونی و یا فضای کسب‌وکار، مانند هتل، پمپ‌بنزین و ...، امکان دسترسی افراد به اینترنت وای‌فای را فراهم می‌کند. شبکه‌های محلی وای‌فای به کامپیوترها و دیگر دستگاه‌ها اجازه برقراری اتصال به اینترنت و همچنین اتصال به یکدیگر، بر روی ارتباطات رادیویی با برد کوتاه و بدون استفاده از سیم را می‌دهند. سیگنال رادیویی از یک نقطه دسترسی وای‌فای، به‌طور معمول از یک رهیاب (مسیریاب بی‌سیم) در یک محل مسکونی پخش می‌شود و هر دستگاهی که قابلیت‌های وای‌فای داشته باشد، می‌تواند به آن متصل شود (Garner, 2004: 1571). حوزه پوشش و سرعت

---

[1]- WLAN

[2]- The How and Why of Wi-Fi, WI-FI ALLIANCE, http://www.wifi. org/knowledge-center/articles/how-and-why-wi-fi (last visited Jan. 7, 2013).

۳- رهیاب واژه مصوب فرهنگستان زبان و ادب فارسی به‌جای Router در انگلیسی و در حوزه رایانه است. روتر (Router) یا مسیریاب‌ها یک تجهیز الکترونیکی فیزیکی (در بعضی از مواقع روترهای نرم‌افزاری در کامپیوتر) در شبکه‌های کامپیوتری هستند که مسؤولیت آن اتصال چندین شبکه به یکدیگر می‌باشد. روتر بسته‌های حاوی اطلاعات را مابین کامپیوترهای شبکه هدایت می‌کند. روترها از روی Header بسته‌ها (Packet) و جداول ارسال‌ها بهترین مسیر را برای ارسال بسته‌ها انتخاب کرده و با استفاده از پروتکل‌ها همانند ICMP با یکدیگر ارتباط برقرار می‌نمایند و بهترین مسیر را مابین دو میزبان پیکره‌بندی می‌کنند. روترها می‌توانند دو شبکه LAN را بهم متصل کنند و یا یک شبکه LAN را به شبکه گسترده WAN امروزه اکثر مودم‌های ADSL در این حال یک روتر نیز به‌حساب می‌آیند و معمولاً بین ۱ تا ۴ پورت LAN و یک پورت WAN را نیز شامل می‌شوند. روترها می‌توانند هم به‌صورت کابل شبکه و یا از طریق بی‌سیم به یکدیگر متصل شوند و اتصال بین شبکه‌ها را برقرار کنند. در شبکه‌های خانگی و یا شرکت‌های کوچک برای متصل‌کردن دو روتر یا مودم ADSL به یکدیگر می‌توان از دو روش استفاده کرد.

اتصال مسیریاب‌های وای‌فای به‌طور چشم‌گیری در چند سال گذشته با به‌کارگیری استانداردهای جدید افزایش یافته است.

در مقابل، رساننده خدمات رایانه‌ای یا رسا که از آن با واژه آی‌اس‌پی به انگلیسی: ISP، مخفف « Internet Service Provider» نیز یاد می‌شود، واسطه دسترسی کاربران به اینترنت است. این شرکت‌ها از خطوط ارتباطی پرسرعت برای دریافت حجم بالای اطلاعات اینترنت و فرستادن داده‌های ارسالی کاربران به سرورها بهره می‌برند و واسطه بین شرکت‌های مخابرات (که دولتی می‌باشند و نقطه تماس بین اینترنت کشور و اینترنت جهانی را ایجاد می‌کنند) و مشترکین اینترنت هستند (Garner, 2004: 953).

در قوانین ایران: «رساها امکان اتصال به شبکه اطلاع‌رسانی و اینترنت را فراهم می‌آورند و جزء ضروری دسترسی و اتصال افراد به شبکه اینترنت هستند. ارائه خدمات تهیه، تولید، توزیع یا ارائه اطلاعات و فراهم‌آوردن امکان دسترسی و همچنین تهیه و فرآوری محتوا برای کاربران از مهم‌ترین فعالیت‌های رسا به‌شمار می‌رود .» آن‌چه از بخش نخست این آیین‌نامه در تعریف ارائه‌کنندگان خدمات اینترنتی پیداست، این است که این بخش، ارائه خدمات دسترسی و اتصال به اینترنت را دربر می‌گیرد و بخش دوم به تعریف ارائه‌کنندگان سایر خدمات چه از سوی خود ارائه‌کننده خدمات در قالب ارائه محتوا و چه توزیع، انتقال و ذخیره اطلاعات برای کاربر می‌پردازد. از دید مقررات خارجی، به‌موجب قانون حق مؤلف هزاره دیجیتال مصوب ۱۹۸۹ ایالات متحده آمریکا ارائه‌کننده خدمات، به مؤسسات و یا شرکت‌های ارائه‌کننده خدمات جهت انتقال اطلاعات و یا ارائه‌دهنده خدمات دسترسی و اتصال جهت ارتباطات برخط دیجیتال میان کاربران برمبنای درخواست‌های کاربران و یا به مؤسسات و شرکت‌های ارائه‌دهنده اطلاعات به انتخاب کاربر بدون هرگونه اعمال ویرایش نسبت به محتوای آن اطلاعات، ارسال و دریافت اطلاعات به همان صورتی که فرستاده و یا دریافت شده است و یا به شرکت‌ها و یا مؤسسات ارائه‌دهندگان خدمات برخط و یا دسترسی به شبکه و یا ارائه‌دهنده خدمات موجود در آن اطلاق می‌شود. قصد بر این بوده است که تعاریف مقرر در این قانون آنچنان گسترده باشند که دانشگاه‌ها و دیگر مؤسسات آموزشی ارائه‌کننده خدمات اینترنتی به دانش‌آموزان، پژوهشگران و دیگر کسان را نیز دربر خود گیرند (ابهری و میری، ۱۳۹۱: ۳).

درنتیجه، تفاوت شبکه‌های وای‌فای محلی که موضوع این مقاله می‌باشند و رساها در این است که برای ایجاد یک رسا نیاز به کسب مجوز از وزارت ارتباطات و فناوری اطلاعات بوده و رسا به‌عنوان واسطه بین مشترکین و فضای اینترنت عمل می‌کند، درحالی‌که یک شبکه بی‌سیم محلی یکی از مشترکین رساها بوده و محدوده پوشش آن، طبق استانداردهای موجود که شرح آن گذشت، نهایتاً ۲۰۰ متر خواهد بود.

۲-۱- فراهم آورندگان خدمات رایانه‌ای و ایجادکننده نقطه تماس بین‌المللی

ایجادکنندگان نقطه تماس بین‌المللی ، مفهوم دیگری است که تفاوت فاحشی با رسا و شبکه وای‌فای محلی دارد. نقطه تماس بین‌المللی معادل فارسی عبارت انگلیسی Access Service Provider یا ASP اصطلاحی است که برای توصیف نوع خاصی از ارائه‌کننده خدمات رایانه‌ای به‌کار می‌رود که رابط بین رساننده‌های خدمات رایانه‌ای به عموم و شبکه جهانی اینترنت است. در ایران مطابق آیین‌نامه نحوه اخذ و ضوابط فنی نقطه تماس بین‌المللی، حق ایجاد آن در انحصار دولت است. در مقابل، یک رسا، خدمات خود را در داخل مرزهای کشور ارائه نموده و از طریق «نقطه تماس بین‌المللی» به شبکه جهانی اینترنت متصل می‌شود. حدود فعالیت ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت رسا به شرح ذیل است:

۱- شرکت‌ها یا مؤسسات ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت رسا تحت ضوابط و قوانین مشخص‌شده در کشور فعالیت می‌نمایند و می‌توانند هم مستقلاً و هم در ارتباط با

۱- آیین‌نامه واحدهای ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت رسا ISP، مصوب ۱۳۸۰.

2- ASP: Acces Service Provider

۳- آیین‌نامه نحوه اخذ و ضوابط فنی نقطه تماس بین‌المللی، شورای عالی انقلاب فرهنگی، مصوب ۱۳۸۰.

شبکه اینترنت به فرآوری اطلاعات پرداخته و به کاربران خود عرضه نمایند؛

۲- ارائه مجموعه خدمات ارزش‌افزوده برخط و برون‌خط برای کاربران خود؛

۳- فراهم‌آوردن دسترسی و همچنین تهیه و فرآوری محتوی برای کاربران خود؛

۴- انجام انواع فعالیت‌ها برای آشنانمودن کاربران در استفاده بهینه از شبکه اطلاع‌رسانی و اینترنت؛

۵- فراهم‌سازی خدمات، تهیه، تولید، توزیع یا ارائه اطلاعات برای کاربران مربوط؛

رساها در سایر کشورها نیز وظایف مشابهی دارند (Wyatt, 2014: 65).

۲- ناامنی شبکه‌های وای‌فای محلی

توسعه حوزه پوشش شبکه‌های وای‌فای این احتمال را افزایش می‌دهد که شخص ثالثی در ساختمان‌ها یا محل‌های مسکونی دیگر، شبکه‌های وای‌فای را شناسایی کرده و امکان بالقوه اتصال به آن را بدون این‌که دیده شود یا مورد شناسایی قرار بگیرد، داشته باشد. امروزه استعمال اصطلاح وای‌فای در معنای موسع، مترادف با هر شبکه بی‌سیم محلی استعمال می‌گردد، اما درحقیقت، وای‌فای یک علامت تضمینی یا دارای استاندارد ثبت‌شده به‌وسیله ائتلاف وای‌فای است و دلالت بر این دارد که این محصول با استانداردهای شماره «802.11» مؤسسه مهندسان برق و الکترونیک مطابقت دارد. باتوجه به این‌که شبکه‌ها بی‌سیم و یا شبکه‌های وای‌فای از نظر موضوع این تحقیق که مسؤولیت ناشی از ناامنی این شبکه‌ها را بررسی می‌کند، دارای تفاوتی مؤثر در موارد مسؤولیت‌زا نیستند و هر دو، امکان اتصال وای‌فای را فراهم می‌کنند، در ادامه از لفظ وای‌فای برای تمامی شبکه‌های بی‌سیم استفاده خواهد شد.

به‌طور ساده، شبکه‌های وای‌فای[۶] می‌توانند به دو روش امن و ناامن عمل نمایند. اتصالات ناامن یا باز شبکه‌های وای‌فای محلی، داده‌های رمزگذاری‌نشده را پخش کرده و اجازه می‌دهند تا کاربران همتا (رومینگ) بدون رضایت و آگاهی قبلی اپراتور یا عامل، از طریق شبکه به اینترنت دسترسی داشته باشند (Kern, 2004: 104). اتصالات امن شبکه‌های محلی وای‌فای نوعی از پروتکل‌های رمزگذاری‌شده را مورد استفاده قرار می‌دهد که از دسترسی دستگاه‌ها به داده‌های پخش‌شده بدون ورود رمز مناسب، جلوگیری می‌کند (Stamp, 2011: 23) در عمل، بیشتر مسیریاب‌های وای‌فای از کارخانه با سیستم امنیتی غیرفعال (یک اسم شبکه و یک نام کاربری و رمز عبور به‌طور پیش‌فرض) برای کاربران فرستاده می‌شوند. این تنظیمات پیش‌فرض برای این طراحی شده‌اند که تنظیمات کاربر نهایی را تا حد ممکن ساده نمایند و شرکت وای‌فای پیشنهاد می‌دهد که تنظیمات پیش‌فرض توسط کاربران شبکه عوض شوند، اما کاربران در بسیاری موارد از همان تنظیمات پیش‌فرض ساده استفاده نموده و اقدام به تغییر تنظیمات پیش‌فرض نمی‌کنند.

این مسأله در حقوق آمریکا به چالش مهمی تبدیل شده است، به‌طور مثال، درحالی‌که هم‌اکنون هفتاد درصد خانواده‌های آمریکایی مسیریاب (مودم)های وای‌فای را نصب کرده‌اند، یازده درصد آن‌ها رمزی که اتصال وای‌فای آن‌ها را محافظت نماید، ندارند و چهار[۴] درصد افرادی[۵] که مورد بررسی قرار گرفته‌اند، اصولاً نمی‌دانند که آیا مسیریاب وای‌فای آن‌ها امن است یا خیر (Watkins, 2013: 8). سؤالی که ممکن است ذهن را مشغول نماید، این است که چرا رساها در زمان ثبت نام مشترک

[1]- On-Line

[2]- Off-Line

[۳]- ماده ۲ آیین‌نامه واحدهای ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت رسا (ISP)، شورای عالی انقلاب فرهنگی، مصوب ۱۳۸۰.

[4]- IEEE: Institute of Electrical and Electronics Engineers

[5]- WI-FI, Registration No.2525795. Available at: http://www.wifi.org/knowledge-center/articles/how-and-why-wi-fi (آخرین بازدید: ۱۳۹۶/۰۸/۲۳).

[۶]- رومینگ در ارتباطات بی‌سیم به‌معنای گسترش خدمات اتصال در مکانی غیر از مکانی که آن خدمات ثبت شده است، می‌باشد. کاربر رویمنگ در این مقاله، کاربری است که در محدوده برد شبکه وای‌فای قرار گرفته و بدون اجازه صاحب آن، به شبکه متصل شده است.

[7]- Security, WI-FI ALLIANCE, http://www.wi-fi.org/discover-and-learn/security (آخرین بازدید: ۱۳۹۶/۰۸/۲۳).

اقدام به امن‌نمودن شبکه نمی‌کنند؟ در پاسخ باید گفت، دلایلی که عاملین یا اپراتورهای شبکه‌های وای‌فای برای ناامن باقی‌گذاشتن اتصالات (مودم‌ها و ...) دارند، متفاوت است. برخی اپراتورهای شبکه‌های محلی وای‌فای باز، تعهدی ایدئولوژیکی مبنی‌بر فراهم‌کردن دسترسی آزاد به اینترنت دارند (Klang & Murray, 2005: 1). برخی اپراتورهای شبکه‌های محلی وای‌فای نیز اتصالات ناامن یا با امنیت ضعیف را برای سازگاری با دستگاه‌های الکترونیکی قدیمی‌تر، حفظ کرده‌اند. این درحالی است که ممکن است برخی مشتریان با فناوری آشنایی نداشته و اصولاً قادر نباشند برای شبکه خود رمز قرار دهند و برخی دیگر ممکن است باوجود داشتن توانایی رمزگذاری شبکه و آگاهی از خطرات ادامه یک اتصال ناامن، صرفاً زمان کافی برای امن‌کردن شبکه خود نداشته باشند.

۳- مسؤولیت اپراتور به‌دلیل سهل‌انگاری در امن‌نمودن شبکه وای‌فای

به‌طور معمول، وکلا در حقوق آمریکا برای محکوم‌نمودن اپراتوری که شبکه وای‌فای خود را ناامن نگه داشته، به جبران خسارات، غالباً موضوع را با یکی از این دو حالت قیاس می‌نمایند: قیاس ناامن نگه‌داشتن شبکه وای‌فای با قراردادن اسلحه پر در دسترس یک کودک سه ساله و یا قیاس آن با جاگذاشتن سوئیچ در خودروی که درهای آن قفل نگردیده است، البته لازم به ذکر است که کارایی این نوع از استدلال و قیاس در مسؤول قلمدادنمودن اپراتور شبکه وای‌فای ناامن محل تردید است. برای مثال مسؤولیت شخصی که اسلحه گرم را در دسترس یک کودک قرار داده و این امر منجر به وقوع حادثه‌ای شده، براساس «نقض وظیفه مراقبت درخصوص کالاهای خطرناک» قابل توجیه است، دلیلی که درخصوص اپراتور شبکه وای‌فای ناامن به‌سختی قابل پذیرش است، زیرا این ادعا که شبکه وای‌فای ناامن به‌سان اسلحه گرم، ازجمله کالاهای خطرناک است، معقول و منطقی نیست (Watkins, 2013: 16).

قیاس اپراتور با شخصی که سوئیچ خودرو را درون آنجا گذاشته و سارقی با آن خودرو منجر به ورود خسارت به دیگری شده است، ظاهر موجه‌تری دارد، اما پذیرش آن با چالش سببیت مواجه است، چراکه جاگذاشتن سوئیچ خودرو در آن سبب نزدیک و بلاواسطه ورود خسارات به ثالث نیست، البته در مواردی نیز بنا به دلایلی نظیر پارک‌کردن خودرو در منطقه جرم‌خیز و یا وجود ریسک ذاتی در عملیات مربوط به وسایل نقلیه موتوری، می‌توان مالک خودرو را مسؤول خسارات وارده از جانب سارق دانسته‌اند (Watkins, 2013: 17). در کل می‌توان گفت قیاس ناامن نگه‌داشتن شبکه وای‌فای به موارد پیش‌گفته، قیاس مع‌الفارق است و برای توجیه مسؤولیت مدنی اپراتور شبکه وای‌فای بایستی به دلایل دیگر روی آورد.

۴- مسؤولیت توأمان ارائه‌دهنده خدمات و استفاده‌کننده

ارائه‌دهندگان خدمات رایانه‌ای معمولاً مقررات مشخصی را در قالب توافقات مکتوب استفاده از خدماتشان درج می‌کنند که استفاده خدمات رایانه‌ای مورد نظر را محدود به یک مودم برای هر خانواده یا شرکت می‌نمایند (Junnarkar, 2004: 73). به‌عنوان مثال، شرکت یاهو در شرایط استفاده از خدمات خود پیش‌بینی نموده که: «کاربرد محدود: شما موافقت می‌نمایید که به هیچ شخص دیگری اجازه استفاده از نام کاربری خود را اعطا نکرده و هریک از زیرمجموعه‌های حساب کاربری می‌بایست صرفاً توسط یکی از اعضای خانواده یا شرکت شما مورد استفاده قرار بگیرد.» مقررات شرکت وریزون نیز مقرر می‌دارد که «شما اجازه نخواهید داشت خدمات با پهنای گسترده را مجدداً به فروش رسانده، آن را برای مقاصد با حجم بالا مصرف نمایید یا به فعالیت‌های مشابهی اقدام نمایید که بارفروش خدمات (تجاری یا غیرتجاری)، به‌نحوی‌که صرفاً توسط شرکت وریزون مقررشده است، محسوب می‌شود. »

[1]- SBC Yahoo!.

۲- برای مثال، ر.ش به شرایط سرویس شرکت یاهو: SBC Yahoo! Terms of Service, SBC Yahoo!, available at: http://sbc.yahoo.com/terms/ (last visited Dec. 8, 2004).

[3]- Verizon

۴- برای مثال، ر.ش به شرایط سرویس شرکت وریزون:
Verizon Internet Access Terms of Service, Verizon, available at http://www2.verizon.net/ policies/tos.asp (last visited Dec. 03, 2004).

ارائه‌کننده خدمات می‌تواند قرارداد مشتریانی که چنین مقرراتی را نقض می‌نماید، فسخ نماید.

برخی قوانین دولتی نیز ممکن است مسؤولیت‌هایی را برای عاملین شبکه‌های وای‌فای که امکان نقض شروط و مقررات خدماتی ارائه‌کنندگان خدمات رایانه‌ای را فراهم می‌نمایند، در نظر گیرند. برای نمونه، ایالت مریلند آمریکا، استفاده از «دستگاه، فناوری یا کالایی که ... برای دسترسی غیرمجاز به ... تبدیل یا تصرف خدمات مخابراتی که توسط یکی از ارائه‌کنندگان خدمات مخابراتی ارائه‌شده مورد استفاده قرار گیرد» را ممنوع نموده است. ایالات دلاویر، فلوریدا، ایلی نویز، میشیگان، ویرجینیا و وایومینگ آمریکا، همگی دارای قوانینی مشابهی هستند (Rasch, 2004: 5). اپراتورها و عاملین دسترسی به وایرلس نیز تا حدی که امکان دسترسی را فراهم نمایند، بدین‌منظور، فعالیت‌های ضرررسان به دیگران را تسهیل نمایند، ممکن است واجد مسؤولیت تلقی شوند. برمبنای فرض اولیه، اگر کسی نسخه‌های غیرمجاز فایل‌های موسیقی را با استفاده از شبکه وای‌فای شخص دیگری بارگیری نماید، بدین‌ترتیب مرتکب نقض کپی‌رایت و حقوق مؤلفین شود، مسؤولیت نقض مزبور ممکن است بر اپراتور شبکه‌های وای‌فای تحمیل شود. همان‌طور که در رأی «ای اند ام[۳]» که متضمن مسؤولیت ناشی از نقض شدید کپی‌رایت توسط یک ارائه‌دهنده شبکه همتا (رومینگ) بود، بیان شده:

«محاکم چنین مسؤولیتی را محدود به قضایایی می‌نمایند که شبکه همتا (رومینگ) حق و توانایی نظارت بر فعالیت فرد ناقض داشته و علاوه‌بر آن نیز منفعت مالی مستقیم در چنین فعالیت‌هایی داشته باشد» (Rasch, 2004: 5). در رابطه با حق و قابلیت نظارت، شبکه‌های وای‌فای خانگی معمولاً دارای مکانیسم‌های نظارتی نیستند که این مسأله ردیابی فعالیت‌هایی که بالقوه ناقض کپی‌رایت هستند را تسهیل می‌نمایند، اگرچه شبکه‌های وای‌فای معمولاً دارای فناوری‌ایی هستند که مشترک را قادر به مسدودنمودن برخی کاربران می‌نماید، اما چنین کارکردهایی معمولاً مستلزم آن است که مشترک، گزینه‌های امنیتی را اعمال نماید که بسیاری از کاربران توانایی اعمال آن را ندارند. از سوی دیگر، باتوجه به این‌که مشترکان وای‌فای خانگی با هدف دسترسی خود به اینترنت وای‌فای و بدون هدف کسب منفعت، اقدام به نصب شبکه می‌کنند، لذا این مشترکین منفعتی در انجام فعالیت‌های ناقض قانون ندارند، البته مشترکین شبکه‌های وای‌فای تجاری ممکن است دارای منافع مالی غیرمستقیمی باشند تا حدی که کاربران ناقض، ممکن است در راستای تلاش‌هایشان برای دانلود بارگیری فایل‌های رسانه‌ای که نقض کپی‌رایت هستند، حق دسترسی بیشتری به این اپراتورها پرداخت نمایند، اما همچنان بی‌میلی غالب به اعمال مسؤولیت بر ارائه‌دهندگان خدمات رایانه‌ای در قبال اعمال خسارت‌باری که توسط کاربران ارتکاب می‌یابند، احتمالاً موجب محافظت و مصونیت آن‌ها از مسؤولیت مشارکتی در این زمینه خواهد بود.

۵- مسؤولیت ناشی از شبکه وای‌فای در حقوق آمریکا

در حقوق ایالات متحده آمریکا، قوانین و مقرراتی که به‌نحو مستقیم به اعمال مسؤولت مدنی بر ناامن نگاه‌داشتن شبکه‌های بیسیم پرداخته باشد، دیده نمی‌شود، اما قواعد مشترکی در قوانین مختلف وجود دارد که در ادامه به بررسی آن‌ها خواهیم پرداخت.

۵-۱- مقررات معافیت از مسؤولیت مقرر در قانون کپی‌رایت هزاره دیجیتال

یکی از مواردی که ممکن است با استفاده از شبکه‌های وای‌فای ناامن رخ دهد و قسمت زیادی از پرونده‌های مرتبط را تشکیل

۱- البته حداقل یکی از شرکت‌های ارائه‌دهنده خدمات رایانه‌ای در ایالات متحده بیان داشته که اقدامات رومینگ غیرقانونی را اصولاً مورد بررسی قرار نمی‌دهد (Junnarkar, 2004: 73).

۲- ر.ش به بخش ۷-۳۱۳ قانون جزای ایالت مریلند آمریکا:
MD. CODE ANN. CRIM. L. § 7-313 (2002). Available at: law.justia.com/codes/maryland/2013/article-gcr/ (آخرین بازدید: ۱۳۹۶/۰۶/۲۲).

۳- ر.ش به رأی صادره در پرونده:
A&M Records, Inc. v. Napster, Inc. 284 F.3d 1091, 1098 (9th Cir. 2002).
در این پرونده که در دادگاه تجدید نظر نیز تأیید شد، دادگاه یک کاربر رومینگ را به‌طور مشترک با دارنده شبکه (مشترک اصلی) مسؤول نقض قوانین کپی‌رایت شناخت.

4- The Linksys Wireless-G Access Point (product number WAP54G) provides features that allow the operator to control who has access to the WLAN, but the product does not support the ability to track or monitor Internet activity.

5- ISP: Internet Service Provider

می‌دهد، سوءاستفاده از شبکه‌های وای‌فای ناامن به‌منظور منتشرنمودن محتوای مشمول حقوق کپی‌رایت است. در این خصوص، قانون کپی‌رایت دیجیتال ایالات متحده آمریکا ارائه‌دهندگان خدمات رایانه‌ای را در زمانی که: «صرفاً به‌عنوان شبکه‌های منفعل عمل می‌کنند یا با کمک ناآگاهانه موجب نقض کپی‌رایت می‌شوند» فاقد مسؤولیت می‌داند (Lesser, 2008: 359)، بر طبق بخش «الف» از ماده ۵۱۲، این مقررات: **«یک ارائه‌دهنده خدمات، به‌دلیل فراهم‌کردن اتصال، انتقال یا مسیریابی مفاد درون سیستم یا شبکه‌ای که (شبکه خانگی) توسط ارائه‌دهنده خدمات نظارت می‌شود یا برای ارائه‌دهنده خدمات کار می‌کند یا به‌دلیل واسطه‌گری یا ذخیره‌سازی موقت مفاد مزبور در حین برقراری اتصال، در قبال غرامت مالی، غرامت قضایی یا دیگر غرامت‌ها برای نقض کپی‌رایت، فاقد مسؤولیت خواهد بود »**، لذا بر طبق این قانون، هیچ مسؤولیتی متوجه ارائه‌دهنده خدمات نمی‌شود تا جایی که:

۱- انتقال (اطلاعات ممنوع) به‌وسیله ارائه‌دهنده خدمات آغاز نشده باشد؛

۲- انتقال، مسیریابی، برقراری ارتباط یا ذخیره‌سازی و ...، به‌طور خودکار و بدون انتخاب مواد به‌وسیله ارائه‌دهنده خدمات انجام شده باشد؛

۳- ارائه‌دهنده خدمات دریافت‌کنندگان مفاد مزبور را انتخاب نکرده باشد؛

۴- نسخه‌ای از مفاد مزبور در سیستم ذخیره و نگهداری نشده باشد (نگهداری کوتاه‌مدت مفاد مزبور در حین برقراری اتصال شامل این بند نخواهد شد)؛

۵- مفاد مزبور از طریق سیستم یا شبکه، بدون اصلاح محتوای آن انتقال داده شده باشد.[۳]

گفته شد که یک ارائه‌دهنده خدمات، نهادی است که خدمات انتقال، مسیریابی، برقراری ارتباط برای ارتباطات آنلاین، در میان یا مابین نقاطی که کاربر مشخص کرده است و از موادی که کاربر انتخاب کرده است را بدون اصلاح و دستکاری محتوای موادی که کاربر فرستاده یا دریافت[۱] کرده است، ارائه می‌دهد.[۴]

درنتیجه، درحالی‌که ارائه‌دهندگان خدمات رایانه‌ای از فعالیت‌های مشترکین خود (با رعایت مقررات قانونی) معاف هستند، شبکه وای‌فای ناامن خانگی یا تجاری که به‌عنوان یک مجرا عمل می‌کند و به هرکس که دارای دستگاه وای‌فای باشد، اجازه دسترسی به اینترنت را می‌دهد نیز می‌تواند یک ارائه‌کننده خدمات رایانه‌ای در نظر گرفته شود، چراکه علاوه‌بر مورد فوق، در این مورد نیز به طرز مشابهی، هرگونه مواد دریافت‌شده یا بارگذاری‌شده ناقض قوانین حق تکثیر، از طریق اتصال به‌وسیله یک کاربر همتا، بدون اطلاع یا دخالت مشترکین شبکه‌های محلی وای‌فای صورت می‌گیرد، لذا دلیلی وجود ندارد که دادگاه‌ها حمایت‌های مقرر در مقررات معافیت از مسؤولیت را در مورد این خواندگان، وقتی که کارکرد آن‌ها اساساً به‌عنوان شرکت‌های کوچک مخابراتی که به کاربران همتا دسترسی به اینترنت ارائه می‌کنند را توسعه ندهند.

البته نقص استدلال فوق مشخص است، چراکه مقایسه مشترکین اینترنت با ارائه‌دهندگان خدمات رایانه‌ای قیاسی مع‌الفارق است، چراکه یک شرکت ارائه‌کننده خدمات، امکان اتصال به شبکه اینترنت را فراهم می‌کند و در واقع واسطه بین مشترکین و اینترنت بوده و در فعالیت خود را در قبال دریافت وجه انجام می‌دهد. این درحالی است که شبکه‌های وای‌فای خانگی یا تجاری، مانند هتل‌ها، رستوران‌ها و ...، خود مشترک رساها بوده و مسافرین هتل یا مشتریان رستوران در واقع افراد تحت پوشش آن‌ها محسوب می‌شوند و نه مشترکین آن‌ها. این مسأله به‌روشنی از تعریف رساها در حقوق ایران و نظریه حقوق‌دانان ایرانی مشخص است. در حقوق ایران: «**رساها امکان اتصال به شبکه اطلاع‌رسانی و اینترنت را فراهم می‌آورند و جزء**

---

[1]- DMCA: Digital Millennium Copyright Act 1988

قانون کپی‌رایت هزاره دیجیتال (DMCA)، یک قانون کپی‌رایت ایالات متحده است که معاهده ۱۹۹۶ سازمان جهانی مالکیت فکری (WIPO) درخصوص حق مؤلف را در حقوق آمریکا قابل لازم‌الاجرا می‌داند.

۲- بخش ۵۱۲ قانون تحدید مسؤولیت نقض آنلاین کپی‌رایت (۲۰۱۶) (Online Copyright Infringement Liability Limitation Act, 17 U.S.C. § 512(a) (2006)).

۳- همان قانون، بخش ۵۱۲، قسمت (5)-(1)(a).

۴- همان قانون، بخش ۵۱۲، قسمت (k)(1)(A).

ضروری دسترسی و اتصال افراد به شبکه اینترنت هستند. ارائه خدمات تهیه، تولید، توزیع یا ارائه اطلاعات و فراهم‌آوردن امکان دسترسی و همچنین تهیه و فرآوری محتوا برای کاربران از مهم‌ترین فعالیت‌های رسا به‌شمار می‌رود. »

در شرح این ماده نیز بیان شده: «**آن‌چه از بخش نخست این آیین‌نامه در تعریف ارائه‌کنندگان خدمات رایانه‌ای پیداست، این است که این بخش، ارائه خدمات دسترسی و اتصال به اینترنت را دربر می‌گیرد و بخش دوم به تعریف ارائه‌کنندگان سایر خدمات چه از سوی خود ارائه‌کننده خدمات در قالب ارائه محتوا و چه توزیع، انتقال و ذخیره اطلاعات برای کاربر می‌پردازد**» (ابهری و میری، ۱۳۹۱: ۴)، لذا معاف‌دانستن شبکه‌های وای‌فای خانگی و تجاری با این عنوان که فعالیت مشابهی با رساها دارند، امری است خلاف نصوص قانونی و منظور قانون‌گذار، چراکه گستردگی فعالیت این دو، ضوابط قانونی فعالیت و خدمات آن‌ها با یکدیگر متفاوت است، به‌نحوی‌که نمی‌توان نظام حقوقی واحدی را بر هر دو اعمال نمود.

۲-۵- مسؤولیت مدنی تحت قواعد عمومی کامن‌لا

ممکن است داشتن شبکه وای‌فای ناامن تقصیر و موجب مسؤولیت تلقی گردد. در قواعد کامن‌لا، به‌طور معمول اقدامات سایبری به دو دسته تقسیم می‌شوند: اقدامات علیه منافع و مصالح شخصی و اقداماتی که علیه اموال و دارایی شخصی ارتکاب می‌یابد (Moore, 2010: 6). خسارات ناشی از اقدامات سایبری که علیه دارایی‌های شخصی صورت می‌گیرد، توسط اکثر حوزه‌های قضایی قابل مطالبه شناخته‌شده است (Moore, 2010: 6). با فرض این‌که، سهل‌انگاری به‌عنوان سبب دعوا علیه مدیر یک شبکه محلی وای‌فای باز به‌دلیل عمل یک شخص ثالث، قابل‌استفاده باشد، وجود تعهد بحث‌برانگیزترین بخش نظریه مسؤولیت است. وکیل خواهان در دعوای «شرکت سوآرم » در سال ۲۰۱۰، این‌گونه استدلال کرد که: استدلال[۲] مطروحه در پرونده «**هوپر** » که بیان داشت «فناوری‌های جدید که مورد استفاده یک فرد معقول قرار می‌گیرد، باید به‌وسیله همه استفاده شود » (Litan, 2011: 158)، به‌منظور شناسایی اصل دسترسی آزاد افراد به اینترنت بوده و در کنار آن، وجود تعهد برای امن[۱]کردن یک مسیریاب وای‌فای، مباینتی با امکان دسترسی آزاد افراد به اینترنت ندارد (Vandall, 2011: 85). استدلال قاضی در این پرونده بر این اساس استوار است که باتوجه به این‌که هزینه امن‌کردن روتر در مقایسه با ضرر بالقوه سوءاستفاده از شبکه ناامن بسیار اندک است، لذا یک شخص معقول باید مسیریاب وای‌فای خود را امن نماید. اصرار بر ناامن باقی‌ماندن شبکه وای‌فای می‌تواند تفریط و موجب مسؤولیت باشد.

این مسأله نشان‌دهنده لزوم تفاوت‌گذاردن میان رساها و مشترکین رایانه‌ای است که شبکه خود را به‌صورت ناامن برای استفاده عموم باز گذارده‌اند و یا شبکه خود را از طریق رمزگذاری امن ننموده‌اند، چراکه امن‌نمودن یک شبکه وای‌فای، در مقام مقایسه با خسارات که به‌سادگی از طریق این شبکه‌های وای‌فای ناامن صورت می‌گیرد، بسیار ناچیز است و می‌توان با اعمال مسؤولیت بر دارندگان این‌گونه شبکه‌ها، به‌سادگی از خسارات مذکور پیشگیری نمود. در عین حال که ناامن باقی‌گذاشتن شبکه وای‌فای می‌تواند تقصیر تلقی گردد. در حقوق کامن‌لا، شرط تحقق بی‌احتیاطی، نقض تکلیفی است که شخص برای احتیاط و مراقبت نسبت به دیگران برعهده داشته است. الگوی احتیاط و مراقبت مبتنی‌بر عملکرد انسان معقول است و این الگوی معیار، برای تعیین مرز بین «آزادی عمل‌خواهان» و «امنیت خوانده» به‌کار می‌رود. الگوی مذکور، نوعی بوده و مطابق با رویه اکثریت مردم است (Cane, 2006: 48-9). این الگو مشخص می‌کند که خوانده در چه مواردی، تکلیف خود به رعایت احتیاط و مراقبت را نقض کرده است. با تکیه بر این الگو، متعارف‌بودن اعمال اشخاص بررسی شده و مشخص[۳] می‌شود که اشخاص چه اعمالی را باید انجام

۱- ماده ۱ آیین‌نامه واحدهای ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت رسا (ISP) مصوب شورای عالی انقلاب فرهنگی، مصوب ۱۳۸۰.

2- Liberty Media Holdings, LLC v. Swarm of Nov. 16, 2010.

3- T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932). U.S. Court of Appeals for the Second Circuit - 60 F.2d 737 (2d Cir. 1932) July 21, 1932

۴- دادگاه در رأی خود بیان داشت: «لزوم مراقبت در این زمینه (شبکه‌های وای‌فای) به قدری اهمیت دارد که نادیده‌گرفته‌شدن این مسأله در سایر کشورها نیز نمی‌تواند اهمیت آن را کاهش دهد» (The T.J. Hooper, 60 F.2d at 740).

۵- این مسأله در رویه قضایی ایالات متحده در پرونده ذیل عنوان شده است: United States v. Carroll Towing Co. 159 F.2d 169, 173 (2d Cir. 1947)

می‌دادند. بنابراین اصولاً این‌که انجام چه عملی در توان آنان بوده و می‌توانستند انجام دهند، از اهمیت برخوردار نیست (Postema, 2002: 43). بدیهی است که اغلب افراد و متعارف افراد شبکه‌های خود را امن نگه می‌دارند.

۶- مسؤولیت ناشی از شبکه وای‌فای در حقوق آلمان

در ابتدا لازم به‌ذکر است که در اتحادیه اروپایی نیز تردیدهای مشابهی با حقوق آمریکا در مورد معافیت شبکه‌های خانگی و تجاری ناامن از مسؤولیت و یا لزوم مسؤولیت ایشان در قبال سوءاستفاده‌های صورت‌گرفته از ناامنی شبکه‌های آن‌ها وجود دارد. با این وجود، یکی از صریح‌ترین اقدامات در زمینه مقابله با شبکه‌های وای‌فای ناامن و دارندگان آن‌ها در آلمان صورت گرفته است. اخیراً دادگاهی در آلمان مقرر نموده که اگر شخصی ثالث، فیلم‌ها، موسیقی یا دیگر فایل‌های صوتی تصویری را به‌نحو غیرقانونی از یک شبکه وای‌فای محافظت‌نشده دانلود و بارگیری نماید، مالک شبکه وای‌فای ممکن است تا ۱۰۰ یورو (معادل تقریبی ۱۲۶ دلار) جریمه شود. پیش از بررسی رأی دادگاه لازم است اشاره شود که جریمه مذکور در وجه دولت بوده و ماهیت جبران خسارت ندارد. به‌موجب رأی دادگاه: «کاربران خصوصی ملزم به کنترل این مسأله هستند که آیا ارتباط وایرلس یا وای‌فای ایشان به نحو مقتضی در برابر خطر سوءاستفاده اشخاص غیرمجاز، جهت ارتکاب نقض کپی‌رایت محافظت‌شده است یا خیر. »

در این پرونده، یک شخص به‌نحو غیرقانونی، موسیقی دانلود نموده و آن را با استفاده از ارتباط وای‌فای شخص دیگری بر روی یک شبکه اشتراک فایل قرار داده است، سپس شخص موسیقی‌دان که حق کپی‌رایت موسیقی مزبور را داشته، اقدام به اقامه دعوا نموده است. در ادامه، اگرچه مالک شبکه وای‌فای توانست اثبات نماید که در زمان وقوع انتقال غیرمجاز موسیقی مزبور در سفر بوده است، اما دادگاه رأی داد که آن‌ها به‌دلیل عدم تأمین امنیت شبکه وای‌فای خود، همچنان در برابر خسارت واردشده مسؤولیت می‌باشند (Watkins, 2013: 665).

به‌طور کلی در زمینه مسؤولیت دارندگان شبکه‌های وای‌فای ناامن با دو سؤال اساسی روبه‌رو هستیم که تا حدودی مربوط به نظم عمومی کشورها هستند: نخست، آیا ما می‌خواهیم که دسترسی آزاد به وای‌فای را تشویق نماییم یا می‌خواهیم شبکه‌های بسته وای‌فای، توسعه یابند؟ مسأله دوم و مهم‌تر برای آینده نظام حقوقی این است که آیا قواعد مسؤولیت می‌بایست به‌نحوی توسعه یابد که وضعیت‌های ایجادشده توسط فناوری وای‌فای را دربر گیرد؟

درخصوص سؤال نخست، سایر ملل این سؤال را به طرق متعدد پاسخ داده‌اند. همان‌طور که دیده شد، در حقوق ایالات متحده تمایل به حفظ دسترسی آزاد وجود دارد. این درحالی است که در حقوق ایران مقررات خاصی درخصوص رمزگذاری شبکه‌های وای‌فای دیده نمی‌شود. آلمان راه میانه معقول‌تری را در پیش گرفته و برای اپراتورهای وای‌فای قراردادن رمز عبور برای محافظت از شبکه‌هایشان را الزامی نموده است. دیوان عالی آلمان در رأی خود بیان داشته: «کاربران خصوصی ملزم به کنترل این هستند که آیا ارتباط وای‌فای ایشان به‌نحو مقتضی در برابر خطر سوءاستفاده اشخاص غیرمجاز جهت ارتکاب نقض کپی‌رایت محافظت‌شده است یا خیر» (Watkins, 2013: 665).

بر طبق رأی دیوان، شبکه‌های وای‌فایی که در ایمن‌سازی شبکه خود قصور بورزند، درصورتی‌که شبکه ایشان توسط شخص ثالثی برای دانلود یا انتشار و اشتراک‌گذاری غیرقانونی محتوای دارای حق کپی‌رایت مورداستفاده قرار گیرد، مشمول جریمه تا ۱۰۰ یورو (۱۳۲ دلار) خواهند بود، اما برای خسارات ناشی از اعمال متخلفانه کاربرانی که اقدامات خود را از طریق

۱- رأی دیوان عالی فدرال موسوم به رمز شبکه اینترنتی بیسیم برای همه، متن رأی در مندرج در:
http://www.billboard.com/biz/articles/news/1206894/germancourt-orderswirelesspasswordsforall. (آخرین بازدید: ۱۳۹۶/۱۱/۲۳)

۲- تصمیم دیوان عالی فدرال آلمان در تاریخ ۲۰۱۰/۱۲ پرونده شماره ۰۸/ ۱۲۱. (Bundesgerichtshof [BGH] May 12, 2010, I ZR 121/08 ¶ 17) قابل دسترس در: https://dejure.org/ (آخرین بازدید: ۱۳۹۶/۱۱/۲۳).

شبکه ناامن صورت داده‌اند، مسؤولیتی نخواهند داشت. در واقع، با اتخاذ این رویکرد، دادگاه تلاش نمود تا میان دو نگرانی بعضاً متضاد هماهنگی ایجاد نماید:

از یک‌سو، باتوجه به این‌که شبکه‌های وای‌فای ناامن، با توسعه و گسترش ارتباط افراد به اینترنت، جامعه را از امکانات متنوع مجازی منتفع سازند (Kern, 2004: 106)، وضع مسؤولیت بر این شبکه‌ها دسترسی و فعالیت قانونمند بر روی شبکه‌های وایرلس را نیز کاهش خواهد داد. از سوی دیگر، مسؤول‌قلمدادنمودن اپراتورهای وای‌فای محافظت و ایمن‌سازی‌نشده در قبال جرایم رایانه‌ای ارتکاب‌یافته توسط کاربران همتا موجب کاهش نقض کپی‌رایت و سایر جرایم رایانه‌ای می‌شود، لذا فقدان هیچ‌نوع مسؤولیتی در این زمینه امری معقول نخواهد بود. بر این اساس دیوان با شناسایی جریمه مالی برای مسؤولین شبکه‌های وای ناامن و عدم شناسایی مسؤولیت برای ایشان در قبال اقدامات تبهکارانه اشخاص ثالث، عملاً موجب گردیده تا صاحبان کسب‌وکار و دارندگان شبکه‌های وای‌فای خانگی تلاش نمایند تا از طرق مختلف، از یک‌سو دسترسی آزاد افراد به شبکه خود را حفظ نمایند و از سوی دیگر با اقداماتی چون فراهم‌آوردن امکان استفاده از طریق دریافت نام کاربری و نام عبور برای مشتریان خود، ریسک انجام فعالیت‌های خلاف قانون با سوءاستفاده از این شبکه‌ها را کاهش دهند. این موضع در راستای تکلیف کلی احتیاط و مراقبت در قانون مدنی آلمان نیز هست. ماده ۸۲۳ قانون مدنی این کشور از «تکلیف احتیاط و مراقبت» سخن گفته است. در این ماده حقوق اشخاص در اجتماع دسته‌بندی شده و در قالب حقوق مربوط به حیات، جسم، سلامت، آزادی، اموال و ... قرار گرفته است. اشخاص مکلفند از تعدی، تفریط و لطمه‌زدن به این حقوق و منافع پرهیز کنند، در غیر این صورت مسؤول خسارات وارده خواهند بود.

۷- مسؤولیت مدنی شبکه‌های وای‌فای ناامن در حقوق ایران

مشکل ناشی از شبکه‌های وای‌فای ناامن، یک چالش جدی در حقوق ایران است. این مسأله با مرور هشدارهای مکرر پلیس فتا و نیروی انتظامی درخصوص امن‌نمودن شبکه‌های وای‌فای محلی و عدم استفاده از شبکه‌های وای‌فای رایگان به‌وضوح آشکار می‌گردد. در حقوق ایران درصورتی‌که شخص ثالثی (شخصی غیر از رسا یا دارنده شبکه وای‌فای محلی) موجب نقض حقوق مؤلف و یا مرتکب جرایم رایانه‌ای شود، چنان‌چه احراز شود ورود خسارت درنتیجه ضعف سیستم یک ارائه‌دهنده خدمات دسترسی یا مانند آن در حفظ امنیت داده‌ها یا محرمانگی آن‌ها یا ضعف سیستم در جلوگیری از انتشار آثار منتشرشده غیرمجاز یا ناقض حقوق کپی‌رایت دیگران بوده، واسطه مزبور که عرفاً و منطقاً انتظار می‌رفت امکانات سیستمی مناسبی را برای جلوگیری از ورود خسارت یا تشدید آن‌ها فراهم نماید، مقصر محسوب شده و باتوجه به ماده ۷۸ قانون تجارت الکترونیک که نقص یا ضعف سیستم مؤسسات خصوصی و دولتی را به‌عنوان تقصیر تلقی نموده و ماده ۱ قانون مسؤولیت مدنی، رسا مسؤول خواهد بود. از سوی دیگر، درصورتی‌که رسا از تکالیفی که به‌موجب قانون برعهده آن گذارده شده، تخطی نماید، مرتکب تقصیر شده و مسؤول تلقی می‌گردد.

اما درخصوص دارندگان شبکه‌های وای‌فای محلی، باتوجه به این‌که فعالیت آن‌ها مشمول ماده ۷۸ قانون تجارت الکترونیک قرار نمی‌گیرند و هیچ نوع جریمه‌ای برای دارندگان شبکه‌های وای‌فای ناامن در نظر گرفته نشده است، اما از حیث مسؤولیت مدنی، باتوجه به این‌که ورود ضرر توسط شخص «الف» (شخصی که از شبکه وای‌فای ناامن استفاده نموده) صورت

۱- تصمیم دیوان عالی فدرال آلمان در تاریخ ۲۰۱۰/۱۲ پرونده شماره ۰۸/ ۱۲۱. (Bundesgerichtshof [BGH] May 12, 2010, I ZR 121/08 ¶ 17)، قابل دسترس در: https://dejure.org/ (آخرین بازدید: ۱۳۹۶/۱۱/۲۳).

2- Section 823 Liability in damages: 1- A person who, intentionally or negligently, unlawfully injures the life, body, health, freedom, property or another right of another person is liable to make compensation to the other party for the damage arising from this; 2- The same duty is held by a person who commits a breach of a statute that is intended to protect another person. If, according to the contents of the statute, it may also be breached without fault, then liability to compensation only exists in the case of fault.

۳- با جستجوی کلمه «اینترنت وای‌فای رایگان» بر روی سایت پلیس فتا، به بیش از پنجاه مورد هشدار در مورد شیوه ارتکاب جرایم با سوءاستفاده از شبکه‌های بی‌سیم ناامن برمی‌خوریم که از سوی پلیس فتا در استان‌های مختلف و به‌دلیل سوءاستفاده مکرر مجرمان از این شبکه‌ها صادر شده است. قابل دسترسی در: https://www.cyberpolice.ir/ (آخرین بازدید: ۱۳۹۶/۰۷/۲۰).

گرفته است، باید دید که آیا ناامن نگه‌داشتن شبکه وای‌فای توسط شخص «ب» می‌تواند مصداق تسبیب در ورود ضرر باشد. در این مورد نکته مهم این است که در بحث تسبیب برخلاف بحث معاونت در جرم که نیازمند وحدت قصد میان مباشر و معاون است، لزومی به وحدت قصد نیست و صرف انتساب عرفی عمل کفایت می‌کند. در این رابطه می‌توان گفت ورود خسارت به غیر با استفاده از شبکه وای‌فای رمزگذاری‌نشده دیگری مصداق اجتماع سبب و مباشر است. ماده ۵۲۶ قانون مجازات اسلامی چنین مقرر داشته است: **«هرگاه دو یا چند عامل، برخی به مباشرت و بعضی به تسبیب در وقوع جنایتی، تأثیر داشته باشند، عاملی که جنایت مستند به اوست، ضامن است و چنان‌چه جنایت مستند به تمام عوامل باشد، به‌طور مساوی ضامن می‌باشند، مگر تأثیر رفتار مرتکبان متفاوت باشد که در این صورت هریک به میزان تأثیر رفتارشان مسؤول هستند، درصورتی‌که مباشر در جنایت بی‌اختیار، جاهل، صغیر غیرممیز یا مجنون و مانند آن‌ها باشد، فقط سبب، ضامن است.»**

اگرچه ظاهراً حکم این ماده، به جنایت منحصر شده است، اما از آنجا که جنایت فاقد خصوصیتی است که قواعد ناظر به تشخیص رابطه استناد منصرف از غیر آن باشد، ضوابط تعیین عامل ضامن بر همه جرایم مقید به نتیجه و کلیه خسارت‌ها و زیان‌های حاصل از دخالت عوامل مختلف در حقوق جزا و حقوق مدنی، حاکم است (صادقی، ۱۳۹۳: ۱۰۳).

سؤالی که باید پاسخ داده شود، آن است که آیا دارنده شبکه وای‌فای ناامن، به‌عنوان سبب، عاملی است که زیان مستند به اوست یا خیر؟ در این رابطه می‌توان به تغییر رویکرد قانون‌گذار در قانون مجازات اسلامی ۱۳۹۲ نسبت به قانون مجازات اسلامی ۱۳۷۰ اشاره نمود. در قانون ۱۳۷۰ مقنن در ماده ۳۶۳ در اجتماع سبب و مباشر، مباشر را مسؤول قلمداد کرده بود، مگر درصورت اقوی‌بودن سبب از مباشر که در این صورت، سبب مسؤول قلمداد گردیده بود، اما در قانون ۱۳۹۲ مقنن این رویکرد را کنار گذاشته و در اجتماع سبب و مباشر، عاملی را مسؤول دانسته که نتیجه مستند به آن باشد، اعم از آن‌که مباشر باشد یا سبب. این رویکرد بیشتر ناشی از این باور است که هیچ‌یک از تئوری‌ها و نظریاتی که درصدد توجیه رابطه استناد هستند، نمی‌تواند به‌طور قاطع بر دعاوی مختلف حاکم باشد و دادرس باید در هر مورد خاص و باتوجه به اوضاع و احوالی که حادثه زیان‌بار را احاطه کرده است، داوری کند. به‌نظر می‌رسد این رویکرد مقنن بیشتر با واقع سنخیت داشته، زیرا همان‌گونه که یکی از نویسندگان برجسته حقوقی اشاره نموده، خسارت را انسان به بار می‌آورد و انسان دیگری درباره آن قضاوت می‌کند. به همین جهت سهم عوامل انسانی را در این راه نباید فراموش کرد و تنها به علم و نظریه‌های فلسفی روی آورد (کاتوزیان، ۱۳۹۰: ۲۸۵/۱). بر این اساس نمی‌توان به‌راحتی به این دلیل که دارنده شبکه وای‌فای ناامن سبب است و سوءاستفاده‌کننده مباشر ورود ضرر، دارنده را مسؤول ندانست و دادرس باید در هر مورد خاص بررسی کرده و درصورت تقصیر دارنده در امن‌نمودن شبکه وای‌فای، وی را مسؤول خسارات قلمداد کند. در مقام تحلیل موضوع می‌توان مسؤولیت مدنی دارنده شبکه وای‌فای را بدین‌نحو تبیین نمود: اعمال مسؤولیت مدنی بر دارندگان شبکه‌های وای‌فای ناامن می‌تواند مبتنی‌بر نظریه تقصیر و یا بدون تقصیر و مبتنی‌بر نظریه خطر باشد:

۱-۷- مسؤولیت بدون تقصیر

مسؤولیت بدون تقصیر دارندگان شبکه‌های وای‌فای ناامن مبتنی‌بر نظریه خطر است. برمبنای این نظر، هرکس که به فعالیتی بپردازد، محیط خطرناکی را برای دیگران به‌وجود می‌آورد و باید خسارت‌هایی را که به دیگران وارد می‌شود، جبران کند، زیرا او است که از منافع آن محیط بهره‌مند می‌شود. در واقع مسؤولیت شخص برای جبران خسارتی که به دیگران وارد می‌کند، به‌خاطر این نیست که او مقصر است، بلکه به‌خاطر سودی است که از ایجاد آن محیط خطرناک به او می‌رسد (عبدالهی بنستانی، ۱۳۹۴: ۱۲۴). برمبنای این نظریه، سرمایه‌داران و صاحبان کارخانه‌ها که از فعالیت‌های خود سود فراوانی می‌بردند، باید خسارات حاصل‌شده از آن را نیز جبران می‌کردند، حتی اگر حوادث ایجادشده به‌خاطر بی‌احتیاطی کارگران رخ می‌داد و یا امکان پیش‌بینی وقوع آن حادثه وجود نداشت (کاتوزیان، ۱۳۸۰: ۲۴).

بر این اساس، وجود ریسک بالای وقوع زیان ناشی از آن عمل، بالابودن میزان زیان رخداده و ناتوانایی عامل برای از میان‌بردن ریسک روی‌دادن زیان، حتی با اجرای اقدامات پیشگیرانه

متعارف مهم‌ترین دلیل بر اعمال مسؤولیت بدون تقصیر بر دارندگان این‌گونه شبکه‌های ناامن است. بر طبق این دیدگاه، دارندگان شبکه‌های وای‌فای محلی ناامن که شبکه‌های خود را به‌خصوص به دلایل تجاری برای کاربران باز گذاشته‌اند (مانند هتل‌ها) باید هزینه مخاطرات ناشی از آن را نیز پذیرا باشند. این دیدگاه مبتنی‌بر تئوری خطر امروزه در مواردی که عمل صورت گرفته نامتعارف باشد، قابل اعمال است (Schruers, 2000: 246) و در حقوق کشورهایی همچون آمریکا نیز اعمال می‌شود (Chueh Chih Yen, 2000: 23).

۲-۷- مسؤولیت مبتنی‌بر تقصیر

در تعریف تقصیر در حقوق کامن‌لا به نظریه انسان معقول و متعارف بیش از همه توجه شده است. از این منظر، انسان معقول کسی است که از ایجاد خطر غیرمعقول و قابل پیش‌بینی منجر به خسارت پرهیز می‌کند. در پرونده بلایت علیه **بیرمنگام** نیز تقصیر این‌چنین تعریف شده است: «تقصیر عبارت است از عدم انجام امری که یک فرد معقول و متعارف در راستای انجام رفتار معمول انسانی در انجام امور انجام می‌دهد یا انجام کاری که یک فرد معقول و متعارف آن را انجام نمی‌دهد» (بیرمنگهام، ۱۳۸۸: ۷۹).

در حقوق موضوعه ایران نیز تقصیر مفهوم عرفی و اجتماعی دارد (امینی و محمدی‌نژاد، ۱۳۹۱: ۱۲). همان‌طور که قانون مدنی در مواد ۹۵۱ تا ۹۵۳ درخصوص تعریف تعدی و تفریط، داوری عرف را در این خصوص پذیرفته است. مناسب‌ترین تعریفی که برای تقصیر به‌نظر می‌رسد، عبارت است از: تعدی و تفریط از رفتار انسانی متعارف در همان شرایط خارجی وقوع حادثه یا رفتاری که هرگاه یک شخص متعارف در شرایط حادثه قرار بگیرد، مرتکب آن نمی‌شود، البته در معیار سنجش مفهوم عرفی تقصیر نیز آن‌چه مورد پذیرش قرار گرفته، مفهوم نوعی و اجتماعی آن است (کاتوزیان، ۱۳۹۰: ۱/۱۹۱-۱۹۰). این تعریف مبتنی‌بر سابقه فقهی موضوع و ارجاع فقها به مفهوم عرفی تقصیر است (موسوی خمینی، ۱۳۶۳: ۲/۵۶۶؛ خویی، ۱۴۲۸: ۲/۲۴۶؛ جبعی عاملی، ۱۳۶۳: ۲۴۵).

حال سؤال اینجاست که آیا عدم رمزگذاری شبکه وای‌فای عرفاً خروج از حد متعارف و یا رفتار انسان معقول تلقی می‌گردد؟ به‌نظر می‌رسد باتوجه به این‌که امن‌نمودن شبکه از طرق معمول همچون قراردادن رمز امری بسیار ساده است که می‌تواند موقعیت‌های متعددی که منجر به وقوع خسارت می‌شود را از بین ببرد، لذا عدم رمزگذاری را می‌توان انجام‌ندادن اقدامی دانست که شخص متعارف انجام می‌دهد (تفریط) و آن را تقصیر تلقی نمود. برای اثبات این مسأله کافی است توجه نمود که هر شخص دارنده شبکه وای‌فای درصورتی‌که بخواهد هم شبکه را در اختیار افرادی که می‌خواهد (مثلاً مشتریان هتل یا رستوران) قرار دهد و در عین حال از سوءاستفاده اشخاص ناشناس از شبکه خود پیشگیری نماید، به سادگی می‌تواند با تعریف کاربران و ارائه نام کاربری مخصوص و پسورد به هر کاربر، به هر دو هدف نائل گردد. درعین‌حال دارندگان شبکه وای‌فای که دارای کاربر مهمان نیستند، مانند شخص که در منزل خود شبکه وای‌فای دارد، می‌تواند با قراردادن رمز در قسمت تنظیمات، از سوءاستفاده‌های احتمالی جلوگیری نماید.

۳-۷- مسؤولیت کیفری

در حقوق ایران، قانون یا مقرراتی که بتوان براساس آن عدم رمزگذاری شبکه وای‌فای را جرم تلقی نمود، وجود ندارد، لذا بر طبق اصل قانونی‌بودن جرایم و مجازات‌ها باید پذیرفت که چنین عملی در حقوق ایران جرم مستقلی نیست و تنها ممکن است با حصول شرایطی همچون تسهیل جرم و وحدت قصد، این عمل را معاونت در جرم دانست که احکام آن مشخص است، لذا جرم‌انگاری غیرامن نگاه‌داشتن شبکه وای‌فای در حقوق ایران نیاز به قانون‌گذاری دارد. از سوی دیگر، باتوجه به بستر مناسبی که شبکه‌های وای‌فای ناامن برای مجرمین ایجاد می‌کنند، به‌نظر نمی‌رسد که صرف وجود مسؤولیت مدنی در این خصوص کافی باشد. شبکه‌های وای‌فای بدون رمزگذاری به‌دلیل عدم امنیت در انتقال داده‌ها و دسترسی آزاد به کاربران ناشناس، می‌توانند بستر مناسبی برای ارتکاب جرایم سایبری شوند. برخی از جرایم شدید مرتبط با این شبکه‌ها عبارتند از:

[1]- Reasonable Man

۱- سرقت هویت و اطلاعات بانکی: یکی از اصلی‌ترین تهدیدات در شبکه‌های وای‌فای بدون رمزگذاری، سرقت هویت است. طبق مطالعات، مجرمان از این شبکه‌ها برای شنود بسته‌های داده استفاده کرده و اطلاعات محرمانه، ازجمله اطلاعات بانکی و هویتی افراد را جمع‌آوری می‌کنند؛

۲- حملات بدافزاری و آلودگی سیستم‌ها: مجرمان از شبکه‌های وای‌فای بدون رمزگذاری برای انتشار بدافزارها استفاده می‌کنند و به دستگاه‌های متصل بدافزار تزریق می‌کنند. مطالعات نشان می‌دهند که حملات «مرد میانی »[1] نیز به‌طور گسترده در شبکه‌های وای‌فای بدون رمزگذاری رخ می‌دهند، جایی که مجرمان بین کاربر و سرویس آنلاین قرار می‌گیرند و اطلاعات انتقال‌یافته را دستکاری می‌کنند؛

۳- پنهان‌شدن مجرمان در شبکه‌های عمومی و خانوادگی: بسیاری از مجرمان از شبکه‌های وای‌فای ناامن برای مخفی‌کردن مکان و هویت خود استفاده می‌کنند، به‌طوری‌که فعالیت‌های غیرقانونی خود را از طریق این شبکه‌ها انجام داده و ردیابی را برای نیروهای پلیس دشوارتر می‌کنند. این امر می‌تواند شامل فعالیت‌های غیرقانونی، مانند خرید و فروش مواد مخدر در فضای آنلاین باشد.

همان‌طور که مشاهده می‌شود، جرایم فوق دارای آثار شدیدی بر اشخاص و جامعه است و نمی‌توان آن‌ها را یک تخلف ساده در نظر گرفت. به‌نظر می‌رسد یافته‌های پیشگیری وضعی مبنای مناسبی برای جرم‌انگاری ناامن نگاه‌داشتن شبکه وای‌فای است، پیشگیری وضعی از جرایم سایبری به‌معنای اعمال روش‌ها و تدابیری است که با تغییر در محیط و کاهش فرصت‌های ارتکاب جرم، مانع از وقوع جرم توسط افراد می‌شود. این رویکرد از تئوری‌های جرم‌شناسی و رفتارشناسی، مانند «نظریه فعالیت‌های روزمره» بهره می‌گیرد و بر این ایده استوار است که با کاهش فرصت‌ها و دسترسی مجرمان به اهداف، می‌توان میزان وقوع جرایم را به حداقل رساند (Clarke, 1995).

در حوزه جرایم سایبری، پیشگیری وضعی با ارتقای امنیت سایبری و کاهش دسترسی مجرمان به شبکه‌های آسیب‌پذیر به‌دست می‌آید. این اقدامات می‌تواند شامل استفاده از رمزگذاری در شبکه‌های وای‌فای، بهره‌گیری از نرم‌افزارهای ضدویروس و تنظیمات امنیتی پیشرفته در شبکه‌های سازمانی و خانگی باشد (Willison & Siponen, 2009). هدف اصلی این رویکرد، ایجاد موانع فنی و عملی برای مجرمان و افزایش هزینه‌های ارتکاب جرم است که آن‌ها را از تلاش برای نفوذ به سیستم‌ها و شبکه‌ها بازمی‌دارد (Newman & Clarke, 2003).

جرم‌انگاری استفاده از شبکه‌های وای‌فای بدون رمزگذاری می‌تواند بخشی از رویکرد پیشگیری وضعی از جرایم سایبری باشد. این اقدام به‌طور مستقیم با هدف کاهش فرصت‌های ارتکاب جرم انجام می‌شود، زیرا شبکه‌های بدون رمزگذاری به‌راحتی قابل نفوذ هستند و می‌توانند به‌عنوان بسترهای ارتکاب جرایم سایبری مورد استفاده قرار گیرند، درنتیجه، الزام قانونی برای رمزگذاری این شبکه‌ها، نه‌تنها امنیت کاربران را افزایش می‌دهد، بلکه دسترسی مجرمان به چنین ابزارهای نفوذپذیری را محدود می‌کند و به کاهش جرایم سایبری کمک می‌نماید. در این خصوص می‌توان مشابه آن‌چه که در حقوق آلمان مشاهده شد، جریمه مالی را به‌عنوان مجازات برای این اقدام در نظر گرفت.

ناگفته نمایند که پیشگیری وضعی در فقه نیز دارای سوابق متعدد است. برخی فقها اقدامات جامعه در برابر بزهکاری را به دو دسته تقسیم کرده‌اند: نخست، اقدامات پیشگیرانه که با هدف جلوگیری از وقوع جرایم انجام می‌شود؛ دوم، واکنش به جرایم گذشته که اساس تصمیم‌گیری قضایی را تشکیل می‌دهد. در سیاست جنایی اسلامی، دفع منکرات همانند رفع آن واجب است، زیرا دلایل وجوب رفع منکر، راهکارهای پیشگیرانه برای جلوگیری از تحقق جرایم و منکرات را نیز شامل می‌شود (میرزافتاح، بی‌تا: ۳۴). نمونه‌های رویکرد مزبور را نیز می‌توان در وجود نهادهایی، همچون حسبه، از بین‌بردن لوازمی که مختص انجام گناه است و اقدامات نظارتی بر

[1]- MITM: Man In the Middle

اشخاص و مکان‌هایی که احتمال بالای وقوع جرم در آن‌ها می‌رود، مشاهده نمود (میرخلیلی، ۱۳۸۳: ۶۹-۶۱)، درنتیجه می‌توان پذیرفت که تعیین جریمه نقدی برای ناامن نگاه‌داشتن شبکه وای‌فای از منظر فقهی نیز با مشکلی روبه‌رو نیست، چراکه علاوه‌بر توجه فقها به پیشگیری وضعی، مشهور فقهای معاصر مجازات مالی را از باب احکام سلطانی مجاز شمرده‌اند (موسوی اردبیلی، ۱۴۲۷: ۶۳/۱؛ موسوی خمینی، ۱۳۹۲: ۵۹۶/۱۰).

نتیجه‌گیری

۱- نظام‌های حقوقی در برخورد با شبکه‌های وای‌فای محلی ناامن با دو چالش عمده روبه‌رو هستند: از یک‌سو بایستی حق دسترسی آزاد شهروندان به اینترنت را تضمین نمایند؛ از سوی دیگر، اقدامات لازم برای پیشگیری از وقوع اعمال خلاف قانون در این حوزه را نیز مد نظر قرار دهند، لذا باتوجه به شیوه توجه به دو مسأله فوق، رویکرد نظام‌های حقوقی به این مسأله متفاوت است؛

۲- در نظام حقوقی آمریکا با این اقدامات در قالب نقض کپی‌رایت و سایر جرایم رایانه‌ای برخورد می‌شود و ناامن‌گذاشتن شبکه وای‌فای، تهدیدی واقعی علیه جامعه تلقی می‌شود و مسؤولیت مدنی ایشان تحت قواعد عام مسؤولیت مدنی کامن‌لا قابل بررسی است. در مقابل، در حقوق آلمان ایمن‌سازی شبکه‌های وای‌فای محلی، تبدیل به یک هدف سیاست‌گذاری ملی شده که طبق آن، ضمن اعمال مسؤولیت بر متخلف اصلی برای خسارات ناشی از عمل وی، مدیران وای‌فای را از طریق جریمه نقدی، تشویق و ترغیب به اتخاذ تدابیر لازم برای ایمن‌سازی شبکه‌هایشان نموده است؛

۳- باتوجه به این‌که بررسی‌های صورت‌گرفته نشان می‌دهد که سوءاستفاده از شبکه‌های ناامن برای ارتکاب اعمال خلاف قانون به‌نحو گسترده‌ای در حقوق ایران نیز صورت می‌گیرد، لازم است تا در این زمینه اقدامی صورت گیرد. به‌نظر می‌رسد که راه حل حقوق آلمان منطقی‌تر از رویکرد حقوق آمریکا به مسأله باشد، زیرا در رویکرد آلمانی، افراد برای ایجاد وضعیتی که ممکن است مورد سوءاستفاده قرار گیرد، جریمه می‌پردازند که این مسأله انگیزه‌های مناسبی را برای امن‌کردن شبکه‌های وای‌فای فراهم می‌کند؛

۴- درنهایت به‌نظر می‌رسد که در حقوق ایران، امکان اعمال مسؤولیت مبتنی‌بر تقصیر بر دارندگان این شبکه‌ها با چالش لزوم احراز رابطه سببیت روبه‌رو است و تنها با استناد به مفهوم عرفی تقصیر می‌توان دارنده این شبکه‌ها را در زیان وارده مسؤول دانست، لذا مسؤولیت مدنی دارندگان شبکه‌های وای‌فای ناامن را از حیث موجبات ضمان باید در زمره تسبیب دانست، چراکه دارنده شبکه وای‌فای به‌صورت مستقیم در بروز زیان دخالت نداشته و تنها سبب آن را فراهم کرده است. تقصیر دانستن ناامن نگه‌داشتن شبکه وای‌فای نیز با استناد به مفهوم عرفی تقصیر که در مقاله مورد اشاره قرار گرفت، امکان‌پذیر خواهد بود. از سوی دیگر، اعمال مسؤولیت جزایی و جزای نقدی نیازمند قانون‌گذاری است که اعمال آن می‌تواند راهکاری در زمینه پیشگیری وضعی از جرایم سایبر باشد، لذا از طریق وضع قانون و اعمال مسؤولیت مدنی می‌توان مالکان را به رمزگذاری شبکه‌ها تشویق و امکان سوءاستفاده از این موقعیت‌ها را حذف نمود و در عین حال، امکان استفاده کاربران را فراهم نگه داشته و تهدیدی به اصل آزادی دسترسی به اینترنت وارد نکرد. این رویکرد در حقوق امریکا نیز از طریق اعمال قواعد عام مسؤولیت مدنی بر دارندگان این‌گونه شبکه‌های ناامن مورد پذیرش است.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانت‌داری در استناد به متون و ارجاعات مقاله تماماً رعایت گردید.

تعارض منافع: تدوین این مقاله، فاقد هرگونه تعارض منافعی بوده است.

سهم نویسندگان: نگارش مقاله به‌صورت مشترک توسط نویسندگان انجام گرفته است.

تشکر و قدردانی: از تمام کسانی که ما را در تهیه این مقاله یاری رسانده‌اند، سپاسگزاریم.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی سامان یافته است.

منابع و مآخذ

الف. منابع فارسی و عربی

– ابهری، حمید و میری، حمید (۱۳۹۱). «پژوهشی تطبیقی پیرامون مسؤولیت مدنی ارائه‌کنندگان خدمات اینترنتی با تأکید بر حقوق آمریکا و اتحادیه اروپا». *مجله پژوهش حقوق خصوصی*، ۱(۱): ۳۸-۱.

– امینی، عیسی و محمدی‌نژاد، سمیرا (۱۳۹۱). «نقش تقصیر در مسؤولیت مدنی و مقایسه آن با حقوق کامن‌لا». *تحقیقات حقوقی تطبیقی ایران و بین الملل*، ۵(۱۸): ۲۲-۱.

– بیرمنگهام، ورا (۱۳۸۸). *شبه‌جرم و مسؤولیت مدنی در حقوق انگلستان*. ترجمه سیدمهدی موسوی، چاپ اول، تهران: انتشارات میزان.

– جبعی عاملی، زین‌الدین (۱۳۶۳). *مسالک الافهام فی شرح شرایع الاسلام*. چاپ اول، قم: انتشارات دارالهدی.

– خویی سیدابوالقاسم (۱۴۲۸). *مبانی تکمله المنهاج*. جلد دوم، چاپ اول، نجف: مطبعه الاداب.

– صادقی، محمدهادی (۱۳۹۳). «اجتماع سبب و مباشر در قانون مجازات اسلامی ۱۳۹۲» *مجله مطالعات حقوقی*، ۶(۲): ۱۲۳-۹۷.

– عبدالهی بنستانی، محمد (۱۳۹۴). «نقش احسان و استیمان در مسؤولیت مدنی». *مجله مطالعات علوم سیاسی، حقوق و فقه*، ۱(۱): ۱۶۷-۹۸.

– کاتوزیان، ناصر (۱۳۸۰). *مسؤولیت مدنی ناشی از حوادث رانندگی*. چاپ اول، تهران: انتشارات دانشگاه تهران.

– کاتوزیان، ناصر (۱۳۹۰). *الزامات خارج از قرارداد، مسؤولیت مدنی*. جلد اول، چاپ اول، تهران: انتشارات دانشگاه تهران.

– موسوی اردبیلی، سیدعبدالکریم (۱۴۲۷). *فقه الحدود و التعزیرات*. جلد اول، چاپ دوم، قم: انتشارات دانشگاه مفید.

– موسوی خمینی، سیدروح‌اله (۱۳۶۳). *تحریرالوسیله*. جلد دوم، چاپ اول، تهران: مکتبه العلمیه الاسلامیه.

– موسوی خمینی، سیدروح‌اله (۱۳۹۲). *موسوعه امام خمینی*. جلد دهم، تهران: مؤسسهٔ تنظیم و نشر آثار امام خمینی.

– میرخلیلی، سیدمحمود (۱۳۸۳). «پیشگیری وضعی از نگاه آموزه‌های اسلام». *مجله فقه و حقوق*، ۱: ۵۹-۷۶.

– میرزافتاح، بیتا (بی‌تا). *هدایه‌الطالب الی اسرار المکاسب*. قم: دارالکتاب.

ب. منابع انگلیسی

- Cane, P (2006). *Atiyah's Accidents, Compensation and the Law*. 7th ed, Cambridge: Cambridge University Press.

- Chueh Chih Yen, A (2000). *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability and the First Amendment*. Boston College Law School Research Paper no.2000-03.

- Clarke, RV (1995). *Situational Crime Prevention*. London: Criminal Justice Press.

- Garner, B (2004). *Black's law Dictionary*. 8th ed, London: Thomson Publication.

- Junnarkar, S (2004). "One Way to Get Online: Piggyback". *New York Times*. Available at: https://www.nytimes.com/2004/08/26/technology/one-way-to-get-online-piggyback.html.

- Kern, B (2004). "Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law, Santa Clara Computer & High Tech". *Santa Clara High Technology Law Journal*, 21(1): 101-162.

- Klang, M & Murray, A (2005). *Human Rights in the Digital Age*. 1st ed, London: Routledge-Cavendish.

- Lesser, L (2008). *Current Copyright Internet Litigation Issues*. 932 PLI/PAT.

- Litan, R (2011). *Handbook on Law, Innovation and Growth*. 2nd ed, Cheltenham: Edward Elgar Publications.

- Moore, R (2010). *Cybercrime: Investigating High-technology Computer Crime*. 2nd ed, New York : Routledge.

- Newman, GR & Clarke, RV (2003). *Superhighway Robbery: Preventing E-Commerce Crime*. London: Willan.

- Postema, G (2002). *Philosophy and the Law of Torts*. 1st ed, Cambridge: Cambridge University Press.

- Rasch, M (2004). *WiFi High Crimes, Security Focus*. Available at: http://www.security focus.com/columnists/237.

- Schruers, M (2002). "The History and Economics of ISP Liability for Third Party Content". *Virginia Law Review*, 88(1): 205-264.

- Stamp, M (2011). *Information Security: Principles and Practice*. 2nd ed, New York: Wiley Publications.

- Vandall, F (2011). *A History of Civil Litigation: Political and Economic Perspectives*. 1st ed, Oxford: Oxford University Press.

- Watkins, C (2013). "Wireless Liability: Liability Concerns for Operators of Unsecured Wireless Networks". *Rutgers Law Review*, Forthcoming, 2013.

- Willison, R & Siponen, M (2009). "Overcoming the Insider: Reducing Employee Computer Crime through Situational Crime Prevention". *Communications of the ACM*, 52(9): 133-137.

- Wyatt, E (2014). F.C.C. in 'Net Neutrality, Turnaround, plans to Allow Fast Lane'. *New York Times*. Available at: https://www.nytimes.com/2014/04/24/technology/fcc-new-net-neutrality-rules.html.