DOI:10.22124/jol.2020.11416.1583

پژوهشنامه حقوق کیفری

سال یازدهم، شماره اول، بهار و تابستان ۱۳۹۹

شماره پیاپی ۲۱

صفحات ۷۴-۵۱

جرایم علیه داده‌پیام‌های شخصی در تجارت الکترونیکی

دکتر علی مراد حیدری[۱]✉

دکتر علی جعفری[۲]

تاریخ دریافت: ۱۳۹۷/۷/۱۴ تاریخ پذیرش: ۱۳۹۸/۳/۲۲

چکیده

نواقص حمایت از داده پیام در ماده ۵۸ قانون تجارت الکترونیکی، ناشی از محدودیت موضوع بـه «داده‌هـای شخصی حساس» و محدودیت رفتارهای مجرمانه به «ذخیره، پردازش و توزیع» است. همچنین، چنـدگانگی قوانین «لازم الاجراء» فعلی و مقررات «ممکن الاجراء» در آینـده ناشـی از پـیش‌نـویس لایحـه «حمایـت از داده‌ها و حریم خصوصی در فضای مجازی» و لایحه «صیانت و حفاظت از داده‌های شخصـی» اسـت کـه در صورت تبدیل به قانون، اعتبار قانون تجارت الکترونیکی و رابطه این مقررات چالش برانگیز خواهد بود.

پرسش اینکه در صورت قانونی شدن این دو لایحه، در موارد خلأ یا تعارض قانونی، کـدام قـانون حـاکم خواهد بود؟ از دید نویسندگان، قاعدهٔ اصولیِ «عام مؤخر ناسخ خاص مقدم نیست» در قلمرو فضای مجـازی ناکارآمد است و راهکار آن کشف «اراده مؤخر قانون‌گذار» است..

واژگان کلیدی: تجارت الکترونیکی، حریم خصوصی، داده شخصی، حریم خصوصی، حمایت از داده

۱. دانشیار گروه حقوق دانشگاه حضرت معصومه(س) ✉ a.m.heydari@hmu.ac.ir

۲. استادیار گروه فقه و مبانی حقوق پردیس فارابی دانشگاه تهران

۱. مقدمه

تجارت الکترونیکی، رفتار انسانی- اجتماعی داد و ستد کالا و خدمات با استفاده از ابزارهای ارتباطی نوین و با مقاصد اقتصادی است. آمارهای خیره کننده‌ای که در برخی از کشورها از حجم تجارت الکترونیکی منتشر شده، حکایت از توسعه بسیار سریع این شیوه از تجارت با بهره‌گیری از سریع‌ترین و ارزان‌ترین فناوری‌های ارتباطی است. برای مثال در سال ۲۰۱۰، حجم تجارت الکترونیکی و خرده فروشی‌ها در ایالات متحده ۱۷۳ میلیارد دلار بود که نسبت به سال ۲۰۰۹، هفت درصد رشد را نشان می‌دهد (السان،۱۳۹۱: ۸).

یکی از چالش‌های اصلی قلمرو تجارت الکترونیکی، مرتبط با حریم خصوصی و داده‌های شخصی و ناشی از این واقعیت است که در این نوع تجارت – بر خلاف تجارت سنتی-، نقش انسان کاهش یافته و بسیاری از مراحل آن از جمله ایجاب و قبول بوسیله فناوری ارتباطی انجام شده و ثمن معامله نیز از طریق پرداخت الکترونیکی مبادله می شود. این امر به نوبه خود زمینهٔ مساعدی برای ذخیره و پردازش داده‌های شخصی افراد در فرایند تجارت الکترونیکی را فراهم می‌آورد.

از سوی دیگر، تجارت الکترونیکی[1] همانند تجارت سنتی- بلکه به طریق اولی- مبتنی بر «بازاریابی»[2] است و اطلاعات مربوط به نیازها، سلیقه‌ها، جنسیت، سن، میزان درآمد، تجربه‌های مصرفی و ...، اطلاعاتی ارزشمند و مؤثر در بازاریابی هستند به گونه‌ای که شرکت‌های تجاری حاضرند برای به دست آوردن آدرس‌ها و ایمیل‌های مشاغل گوناگون هزینه‌های بالایی پرداخت نمایند که گرچه هر یک از این اطلاعات شخصی به تنهایی ممکن است ارزش ویژه‌ای نداشته باشد، لکن پردازش، تلفیق و نگهداری مجموعه‌ای از این اطلاعات منجر به ترسیم نموداری بسیار دقیق از فرد یا افراد مورد نظر می‌گردد و انباشته شدن آنها در پرونده ها و پایگاه‌های اطلاعاتی و پردازش آنها سایه‌ای از هراس مداوم پدید می‌آورد که تهدیدی جدی علیه حریم خصوصی است و هر لحظه ممکن است موجب فرو ریختن ستون‌های محرمانگی و حیثیت و آبروی افراد گردد(محسنی، ۱۳۸۹: ۳۳۷). از این روی، یکی از مهم‌ترین تهدیدات تجارت الکترونیکی، تعرض نسبت به داده‌های پیام‌های شخصی و حریم خصوصی افراد است.

از منظر آموزه‌های اسلامی، مردم و مسئولان حکومتی از پایش و نقض حریم خصوصی افراد منع شده‌اند. قرآن کریم مردم را از کنجکاوی و سرک کشیدن و جستجوی عیوب دیگران منع کرده است[3] و رسول خدا در آخرین خطبه ایراد شده در مدینه فرمودند: هر کس در راه جستجوی عیوب

1. Electronic Commerce
2. Marketting
۳. « یا أیها الذین آمنوا اجتنبوا کثیراً من الظن انّ بعض الظن اثمٌ و لاتجسّسوا» (حجرات/ آیه ۱۲)

و کشف لغزش‌های برادرش گام نهد، پای در آتش دوزخ گذارده و خداوند عیوب او را برهمگان آشکار خواهد کرد.[۱] عمر بن حنظله می‌گوید: به امام صادق(ع) عرض کردم: بازنی ازدواج کرده‌ام، از حال او پرسیدم، گفتند: در عده است. امام(ع) فرمود: چرا از حال او پرس‌و جو کردی؟! بر شما تفتیش لازم نیست(خرازی، ۱۳۸۰: ۶۱).

در سطح بین‌المللی بند ۱ ماده ۱۷ میثاق حقوق مدنی ـ سیاسی مصوب ۱۹۶۶[۲]، بند ۲ اعلامیه کنفرانس حقوقدانان درباره حق رعایت حریم خصوصی[۳]، ماده ۱۴ کنوانسیون ملل متحد درباره کارگران مهاجر[۴]، ماده ۱۶ کنوانسیون ملل متحد در حمایت از کودکان[۵]، ماده ۳۵ بیانیه اصول اجلاس عالی سران درباره جامعه اطلاعاتی مصوب ۱۲ دسامبر ۲۰۰۳ [۶]، بند اول ماده ۸ کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های اساسی سال ۱۹۵۰[۷] و ماده ۱۱ کنوانسیون آمریکایی حقوق بشر[۸]، حریم‌خصوصی مورد توجه قرار گرفته است. در اعلامیه حقوق بشر اسلامی مصوب ۱۴ محرم ۱۴۱۱ قمری در قاهره[۹] نیز در ماده ۱۸ قسمت «ب» در راستای توجه به حریم خصوصی آمده است: «هر انسانی حق دارد که در امور زندگی خصوصی خود در مسکن، خانواده، مال و ارتباطات استقلال داشته باشد و جاسوسی یا نظارت بر او یا مخدوش کردن حیثیت او جائز نیست و باید از او در مقابل هرگونه دخالت زورگویانه در این شئون حمایت شود.»(مهرپور، ۱۳۸۸: ۵۷۳) از دیگر کنوانسیون‌های منطقه‌ای در این ارتباط می‌توان به کنوانسیون شورای اروپا راجع به حمایت از حقوق بشر و آزادی‌های اساسی مصوب ۱۹۵۰[۱۰]، کنوانسیون شورای اروپا راجع به حق حریم خصوصی مصوب ۱۹۸۰[۱۱]، دستورالعمل اتحادیهٔ اروپایی در مورد حمایت از داده‌ها مصوب ۱۹۹۵[۱۲]، اشاره کرد که به طور عام بر مقولهٔ حق حریم خصوصی تأکید کرده‌اند.

---

۱. من مشی فی عیب اخیه وکشف عورته کان اول خطوهٔ خطاها ووضعها فی جهنم وکشف الله عورته علی رووس الخلائق(خرازی، ۱۳۸۰: ۶۱)

2. Civil and Political Rights Covenant.
3. Declaration of the Conference of Lawyers on the Right to Privacy.
4. United Nations Convention on Migrant Workers.
5. United Nations Convention on the Protection of Children.
6. Statement of Principles of the Summit on the Information Society.
7. European Convention for the Protection of Human Rights and Fundamental Freedoms.
8. American Convention on Human Rights.
9. Islamic Human Rights Declaration.
10. Council of Europe Convention on the Protection of Human Rights and Fundamental Freedoms.
11. Council of Europe Convention on the Right to Privacy.
12. European Union Guidelines on Data Protection.

با وجود مباحث فراوانی که در مورد حریم خصوصی مطرح شده است، به نظر می‌رسد مسائل اساسی وجود دارد که حمایت از حریم خصوص را با چالش مواجه کرده است. اولین مسأله، ابهام در مفهوم حریم خصوصی و مشکل تعیین دامنه این موضوع است به گونه‌ای که به گفته ویلیام بی نی حتی جدی‌ترین مدافعان حریم خصوصی باید اعتراف کنند که مشکلات جدی در تعریف ذات و قلمرو این حق وجود دارد(انصاری،۱۳۸۶: ۱۲) و اختلاف در مفهوم، تعیین قلمرو مصداقی این حق را هم دچار مشکل می‌کند بنابراین پاسخ به پرسش‌هایی از این دست که ملاک تعیین حریم خصوصی شخصی است یا نوعی؟ نفی و اثبات حریم خصوصی با اراده صاحب حق رابطه‌ای دارد یا خیر؟ آیا حریم خصوصی ارزش مالی دارد یا نه؟ در اماکن عمومی هم حریم خصوصی قابل تصور است یا نه؟ رابطه حریم خصوصی با علن چیست و آیا حریم خصوصی با پنهانی بودن ملازمه دارد یا نه؟ آیا حضور تعداد زیادی از افراد یا آگاهی تعداد زیادی از افراد از یک موضوع، آن را از حیطه خصوصی بودن خارج می‌کند یا خیر؟ و ده ها پرسش از این دست بستگی به این دارد که چه تعریفی از حریم خصوصی داشته باشیم.[1]

مسأله دوم، استثنائات حریم خصوصی و مبانی توجیه‌کننده نقض حریم خصوصی است که رابطه مستقیمی با ارزش‌های فرهنگی و اجتماعی و نظام حقوقی جوامع مختلف دارد. و هر پاسخی نیز به رویکرد فلسفی در مورد مبنا و قلمرو دخالت حکومت در امور شهروندان دارد و رابطهٔ معناداری بین مبانی دخالت دولت و قلمرو حریم خصوصی وجود دارد به گونه‌ای که در نظام‌های حقوقی مبتنی بر دیدگاه‌های آزادی خواه و فردمحور، فلسفه جرم انگاری و دخالت دولت در امور شهروندان بیشتر مبتنی بر اصل «عدم اضرار به غیر» و به ندرت مبتنی بر اصل پدرسالاری حقوقی و یا اخلاق‌گرایی حقوقی است(کوهن، ۲۰۰۰: ۸۶). در حقیقت چنین رویکردی، خواهان دخالت حداقلی دولت در حریم خصوصی است. در چنین دیدگاه‌هایی وظیفه قوانین جزا، حفظ نظم و آداب عمومی برای حفظ شهروندان از آسیب و تجاوز به آنان و نیز فراهم کردن زمینه‌ای مطمئن در برابر بهره‌کشی از دیگران و به فساد کشیدن آنان است و نه دخالت در زندگی خصوصی شهروندان و تحمیل الگوی رفتاری خاص. پس قلمروی از اخلاق خصوصی وجود دارد که در حیطه وظیفه قانون نمی‌باشد(تبیت، ۱۳۸۴: ۱۷۸).

---

۱. در بند اول از ماده ۲ طرح حریم خصوصی این تعریف برای حریم خصوصی برگزیده شده است: «حریم خصوصی: قلمرویی از زندگی هرشخص است که آن شخص عرفاً یا با اعلان قبلی در چارچوب قانون، انتظار دارد تا دیگران بدون رضایت وی به آن وارد نشوند یا بر آن نگاه یا نظارت نکنند و یا به اطلاعات راجع به آن دسترسی نداشته یا در آن قلمرو وی را مورد تعرض قرار ندهند. جسم، البسه و اشیاء همراه افراد، اماکن خصوصی و منازل، محلهای کار، اطلاعات شخصی و ارتباطات خصوصی با دیگران حریم خصوصی محسوب می‌شوند.»

اما در دیدگاه‌های جامعه محور یا دیدگاه‌های مبتنی بر ایجاد تعادل بین حقوق فرد و جامعه، مبانی دخالت دولت در امور شهروندان متعدد بوده و به تبع آن، قلمرو حریم خصوصی محدودتر خواهد شد و زمانی‌که حمایت از منافع امنیتی، اقتصادی، اخلاقی، بهداشتی و رفاهی جامعه به‌عنوان عواملی برای دخالت دولت و وضع قانون به شمار رود[1]، نتیجه آن امکان محدود شدن حریم خصوصی است و اینجاست که رویکرد مقنن در فرض تزاحم حقوق فردی و حقوق جامعه مبنی بر نحوه ایجاد تعادل بین دو حق بسیار حساس و تعیین‌کننده است و هرگونه ترجیح منافع عمومی بر حقوق فردی، موجب محدود شدن حریم خصوصی خواهد شد.

در نظام حقوقی ایران همپوشانی مقررات مربوط به حمایت از داده پیام‌های شخصی، یک چالش خودساخته به شمار می‌آید. از یک سوی قانون تجارت الکترونیکی مصوب ۱۳۸۲/۱۰/۱۷، با جرم انگاری تعرض به داده‌های شخصی افراد در بستر معاملات الکترونیکی، حریم خصوصی آنان را مورد حمایت کیفری قرار داده است. و از سوی دیگر، در دی ماه ۱۳۹۶ پیش نویس «لایحه حمایت از داده و حریم خصوصی در فضای مجازی»[2] و در تیرماه ۱۳۹۷ پیش‌نویس لایحه «صیانت و حفاظت از داده‌های شخصی»[3] تهیه و برای اظهار نظر علمی در اختیار صاحبنظران قرار گرفته است که در

---

۱. در بند دوم ماده ۸ کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های اساسی سال ۱۹۵۰، تصریح شده که هیچ مقام دولتی نباید به استفاده از این حق تعرض کند، مگر مطابق قانون و در صورتی که این کار برای امنیت ملی، سلامت عمومی یا رفاه اقتصادی کشور، پیشگیری از جرم و بی‌نظمی ، سلامت اخلاقی، یا برای حمایت از حقوق و آزادی‌های دیگران، در یک جامعه دموکراتیک ضروری باشد. (پلومان،۱۳۸۰: ۲۵۰)

۲. لایحه حمایت از داده و حریم خصوصی در فضای مجازی که به همت سازمان فناوری اطلاعات ایران و پژوهشگاه قوه قضاییه و دانشگاه علم و فرهنگ تدوین و در دهم دی ماه ۱۳۹۶ منتشر شده است، یکی از مهمترین لوایح در خصوص حفظ حریم خصوصی و صیانت از داده ها و اطلاعات کاربران در حوزه فضای سایبر است. با وجود کوشش فراوانی که در تهیه متن پیش نویس صورت گرفته، همچنان دارای اشکالات شکلی و ماهوی از جمله عدم حفاظت از اطلاعات مخصوصاً اطلاعات مالی است. به نظر می رسد به جهت اشکالات فراوان پیش نویس، زمان بیشتری جهت نقد آن از سوی صاحبنظران لازم بوده و تاکنون هیچگونه اقدام رسمی در خصوص آن صورت نگرفته است و چه بسا در صورت قانون شدن لایحه «صیانت و حفاظت از داده‌های شخصی» از اهمیت و ضرورت تصویب این آن کاسته شود.

۳. پیش نویس «لایحه صیانت از داده‌های شخصی» به پیشنهاد وزارت ارتباطات و فناوری اطلاعات به توسط سازمان فناوری اطلاعات تدوین و در تیرماه ۱۳۹۷منتشر و سپس به کمیسیون فرعی حوزه دولت الکترونیک ریاست جمهوری ارجاع شد تا نهادهای مربوطه پیش نویش این لایحه را بررسی کنند. اوایل سال ۱۳۹۸ نسخه نهایی این لایحه آماده و اکنون این نسخه به کمیسیون اصلی حوزه دولت الکترونیک ارسال شده تا در هیأت وزیران تصویب شود. از سوی دیگر لایحه«صیانت و حفاظت از داده‌های شخصی» همزمان به صورت طرح نیز به مجلس رفته است و به گفته یکی از اعضای کمیته فضای مجازی کمیسیون فرهنگی مجلس بررسی این طرح از دوشنبه ۲۳ اردیبهشت ماه در کمیسیون فرهنگی مجلس مورد بررسی قرار گرفته تا درباره تمام بندها و بخش‌های آن بحث شود، لکن تا زمان این نوشتار هنوز بررسی این لایحه به پایان نرسیده است.

صورت تبدیل شدن آن به قانون، کشف قانون حاکم در موارد خلأ یا تعارض در حمایت از داده پیام‌های شخصی، از اهمیت بالایی برخوردار خواهد بود.

در این نوشتار، ضمن توصیف ارکان و عناصر جرم «نقض داده پیام‌های شخصی در تجارت الکترونیکی»، نقاط ضعف و قوت آن را با رویکردی تحلیلی، در پرتو مقررات موجود، مورد نقد و ارزیابی قرار گرفته است.

۱. رکن قانونی

رکن قانونی این جرم، ماده ۵۹ قانون تجارت الکترونیکی است که مقرر نموده است: «ذخیره پردازش و یا توزیع داده پیام‌های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و داده پیام‌های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آن‌ها به هر عنوان غیر قانونی است.» ضمانت اجرای این عمل نیز در ماده ۷۱ این قانون تعیین و اعلام شده است: «هر کس در بستر مبادلات الکترونیکی شرایط مقرر در مواد ۵۸ و ۵۹ این قانون را نقض نماید مجرم محسوب و به یک تا سه سال حبس محکوم می‌شود.» همچنین برابر ماده ۲۹ پیش‌نویس لایحه پیش گفته: «هر کس به‌طور غیرمجاز داده های شخصی دیگران را ایجاد، جمع‌آوری، پردازش یا استفاده کند، به جزای نقدی درجه ۶ محکوم خواهد شد. در صورتی که مرتکب این اقدامات را به قصد انتفاع مالی خود یا دیگری انجام داده باشد یا از این طریق موجب وارد شدن ضرر مالی یا حیثیتی به دیگری شده باشد به مجازات حبس و جزای نقدی درجه ۶ محکوم خواهد شد. تبصره ۱: هر گاه داده های شخص، حساس باشد یا داده های شخصی بطور غیرمجاز در اختیار دیگری قرار داده شده یا منتشر شده باشد حسب مورد، مرتکب به حداکثر مجازات مقرر محکوم خواهد شد.» و برابر ماده ۶۸ پیش‌نویس لایحه «صیانت و حفاظت از داده‌های شخصی» مرتکبان ذیل به مجازات مقرر محکوم می‌شوند: **الف)**نقض حق رضایت شخص موضوع داده، چنانچه داده‌های وضعیت‌ها و موقعیت‌های غیرعمومی پردازش شود، به مجازات درجه ۵ و چنانچه داده‌های وضعیت‌ها و موقعیت‌های عمومی پردازش شود، به مجازات درجه ۶؛ **ب)**ممانعت ازاستیفای همه یا بخشی از حق درخواست شخص موضوع داده درباره پردازش یا توقف آن یا انجام پردازش داده‌های شخصی به‌وسیله خود وی یا نقض حق گمنامی، به یک یا دو مجازات درجه ۶؛ **پ)** نقض تعهدات اعتبارپذیری، اعتمادپذیری یا استنادپذیری پردازش داده‌های شخصی، به یک یا دو مجازات درجه ۵ ...» و برابر ماده ۶۹ این لایحه، در شرایطی، مجازات مرتکب یک یا دو درجه بالاتر تعیین می‌شود.

فلسفه جرم انگاری مداخله و تعرض به داده پیام های شخصی، مقابله با سوء استفاده از این

اطلاعات در جریان بازاریابی مستقیم است. چرا که امروزه با استفاده از نرم‌افزارهای طراحی شده در رایانه شخصی کاربر، امکان کشف علایق و سلایق طیف‌های مختلف مصرف کنندگان در نقاط مختلف و آگاهی یافتن از نیاز بازار وجود دارد. اهمیت این موضوع تا جایی است که گاه عرضه کنندگان خدمات اینترنتی یا اداره کنندگان سایت‌ها اقدام به جمع‌آوری اطلاعات از کاربران در حین گشت و گذار در وب و فروش آن به موسسات تجاری می‌نمایند. بازاریابان برخط بهترین مشتریان این اطلاعات هستند و با استفاده از آن به تدوین استراتژی‌های بازاریابی و پیدا کردن بازار هدف خود می‌پردازند.

بسیاری از پایگاه‌های اینترنتی نیز بطور خودکار اقدام به نصب ردنما بر روی رایانه کاربر می‌کنند. پاره‌ای از این ردنماها تنها برای ردیابی کاربران در یک پایگاه معین طراحی شده‌اند ولی بعضی دیگر همه فعالیت‌ها را در شبکه جهانی اینترنت و تمام پایگاه‌های اینترنتی ردیابی می‌کنند. افزون بر این، هنگامی‌که کاربر از صفحات مختلف پایگاه اینترنتی دیدار می‌کند، رایانه شخصی او نسخه‌ای از آن صفحات را ذخیره می‌کند به‌گونه‌ای که دسترسی و پایش رایانه شخصی افراد، به روشنی پایگاه‌های مورد علاقه آنان را مشخص خواهد کرد.

۲. رکن مادی

اجزای رکن مادی جرم نقض داده پیام‌های شخصی شامل موضوع، رفتار، نتیجه و بستر وقوع جرم به شرح زیر است:

۲. ۱. موضوع جرم

موضوع جرم، داده پیام‌های شخصی حساس است. این عنوان دارای سه قید به شرح زیر است که باید بررسی شود:

۲. ۱. ۱. داده پیام

داده پیام، به معنای اطلاعاتی است که قابلیت پردازش توسط سامانه و برنامه رایانه‌ای را دارد(جعفری، ۱۳۹۶: ۳۹ تا ۴۱). در بند ب ماده ۱ کنوانسیون جرایم سایبری آمده است: «داده رایانه‌ای هر گونه نماد حقایق، اطلاعات یا مفاهیم به شکلی مناسب برای پردازش در یک سیستم رایانه‌ای است که برای کارکرد یک سیستم رایانه‌ای مناسب است.» عبارت «مناسب برای پردازش» حاوی این پیام است که داده ها به شکلی وارد می‌شوند که بتوان آنها را به‌صورت مستقیم به-وسیله سیستم رایانه‌ای پردازش کرد(جلالی فراهانی، ۱۳۸۹، ص۲۰).

۲. ۱. ۲. داده پیام شخصی

مراد از داده پیام شخصی عبارت است از اطلاعات مربوط به شخص معین. بر اساس بند ۲ دستورالعمل اتحادیه اروپا برای حمایت از داده‌ها، «داده‌های شخصی داده‌هایی است که درباره یک شخص حقیقی قابل شناسایی یا شناسایی شده باشد»(کنیون، ۱۳۹۶: ۱۹۶) بند (ر) ماده (۲) قانون تجارت الکترونیکی داده پیام‌های شخصی را به معنای «داده پیام‌های مربوط به یک شخص حقیقی موضوع داده (Data Subject) مشخص و معین» دانسته است. این تعریف چندان روشن نیست در حالی‌که بند اول ماده ۱ پیش‌نویس لایحه پیش گفته داده شخصی را «داده‌ای که به‌وسیلهٔ آن به تنهایی یا به همراه داده‌های دیگر بتوان شخص موضوع آن را شناسایی کرد» تعریف کرده است. برابر بند ۴ ماده ۲ طرح حمایت از حریم خصوصی داده پیام‌های شخصی عبارت است از: «اطلاعات وابسته به شخصیت افراد نظیر وضعیت زندگی خانوادگی، عادت‌های فردی، ناراحتی‌های جسمی و شماره کارت‌های اعتباری و شماره حساب‌های بانکی و ...» در تبصره این ماده نیز تصریح شده که «اطلاعات مربوط به نام و نام‌خانوادگی، نشانی‌های محل سکونت و محل کار و شماره‌های تلفن از شمول تعریف اطلاعات شخصی خارج می‌باشد.» این در حالی است که دادگاه اتحادیه اروپا اطلاعات شماره تلفن، اطلاعات شرایط کار و عادات را از مصادیق داده‌های شخصی دانسته است(لاداتی و آرین، ۲۰۱۶: ۳۸).

۲. ۱. ۳. داده پیام شخصی حساس

البته مطلق داده پیام‌های شخصی موضوع جرم ماده ۵۸ نیست بلکه داده پیام مقید به قید «حساس» بودن است. طبق آنچه در بند ۵ ماده (۲) طرح حمایت از حریم خصوصی آمده: «اطلاعات شخصی حساس، اطلاعات راجع به وضعیت زندگی جنسی، اعتقادات (اعم از فلسفی، مذهبی و سیاسی) عضویت در احزاب یا تشکل‌های صنفی و وضعیت نژادی، قومی و قبیله‌ای افراد است»(اداره کل قوانین، ۱۳۸۵: ۵۶۰) ایراد اساسی در این زمینه سیال بودن مفهومی اصطلاحات به‌کار رفته و انعطاف پذیری و قابلیت تسری به هر گونه اطلاعاتی حتی اطلاعات مربوط به عضویت در تشکل صنفی است که ویژگی خاص یا پیامدهای خاصی برای فرد ندارد. از سوی دیگر برابر بند ۲ ماده ۱۵ پیش نویس لایحه مورد بحث، «داده‌های مرتبط با عقاید سیاسی، حزبی، فلسفی، دینی یا مذهبی، قومیت، وضعیت جسمانی، رفتارهای جنسی، اتهامات و محکومیت‌های کیفری داده شخصی حساس محسوب می‌شود» این تعریف نیز دارای اشکالاتی است؛ اولاً به نظر می‌رسد مصادیق داده‌های حساس برگردان قوانین بین‌المللی مانند آنسیترال است و ناظر به جوامعی است که گرایش‌های دینی و مذهبی در ایفای نقش‌های اجتماعی تأثیری ندارد در حالیکه در ایران گرایش دینی و مذهبی در احراز صلاحیت‌ها یا اشتغال به مشاغلی مانند قضاوت موثر است و حتی

ازدواج و طلاق و احوال شخصیه نیز مرتبط با دین و مذهب است و دسترسی و گاه اعلام آن ناگزیر است؛ ثانیاً با وجود برخی ایرادات وارد بر تشهیر رسانه‌ای(حیدری، ۱۳۹۲: ۱۳۹)، در حال حاضر برابر ماده ۳۶ قانون مجازات اسلامی انتشار حکم محکومیت در بعضی موارد به حکم قانون به عنوان یک مجازات توسط مراجع قضایی انجام می‌گیرد از این روی ۳-۴ ماده ۱۵ پیش نویس ایجاد یا پردازش یا استفاده از داده‌های شخصی حساس را «در صورتی که برای کشف جرم یا اجرای مجازات ضروری باشد» مجاز دانسته است.

با وجود این و با توجه به تعریف اطلاعات شخصی حساس در طرح حمایت از حریم خصوصی و پیش نویس لایحه حمایت از داده‌ها و مقایسه آن با مصادیق مذکور در ماده ۵۸ قانون تجارت الکترونیکی، به نظر می‌رسد موضوع جرم ماده ۵۸ از دو جهت ناقص است؛ از یک سو موضوع جرم محدود به اطلاعات «شخصی» است و بر خلاف ماده ۶۶۹ قانون مجازات اسلامی(تعزیرات) و ماده ۲۰۴ قانون مدنی، از اطلاعات خصوصی غیرشخصی – حتی اگر اطلاعات از وصف حساسیت هم برخوردار باشد- حمایتی به عمل نیامده است.

مراد از اطلاعات خصوصی غیر شخصی، اطلاعات خصوصی مربوط به نوامیس و بستگان نزدیک فرد است که گرچه این اطلاعات نسبت به خود آن فرد، «شخصی» محسوب نمی‌شود، لکن در زمره داده‌هایی است که افشای آنها به منسوبٌ الیه هم لطمه وارد کرده و موجب ضرر شرافتی و حیثیت به وی می‌گردد. مشابه این بحث در مورد اکراه و تهدید به ضرر به بستگان – یعنی کسانی که ضرر به آنها به ضرر و تألم شخص منجر می‌گردد- مطرح شده و فقها تهدید به ضرر نسبت به اشخاصی که جاری مجرای خود شخص هستند مانند پدر و فرزند را، محقِّق اکراه می‌دانند.(علامه حلی، ۱۴۱۰ ق، ج۲: ۴۲ ؛ شهید ثانی، ۱۴۱۳ ق، ج ۹: ۱۷)؛ از سوی دیگر، مطلق اطلاعات شخصی نیز موضوع جرم نیست، بلکه موضوع جرم منحصر به داده‌های شخصی «حساس» است و بدین ترتیب تعرض به اطلاعات شخصی فاقد این قید - مانند اطلاعات مربوط به شغل، محل سکونت، منابع و درآمدهای مالی و حساب‌های بانکی و حتی بسیاری از امور خانوادگی-، موضوع این جرم نخواهد بود.

این در حالی است که برابر ماده ۲۹ پیش نویس لایحه، داده‌های شخصی اعم از حساس و غیرحساس موضوع جرم قرار گرفته و حساس بودن داده‌های مورد تعرض تنها موجب تشدید مجازات است و به نظر می‌رسد از آنجا که پیش نویس لایحه نسبت به ق.ت.ا. عام است و در خصوص داده‌های شخصی غیرحساس تعارضی بین دو مقرره نیست، در صورت قانون شدن پیش‌نویس لایحه باید به آن استناد کرد.

۲. ۲. رفتار مجرمانه

رفتارهای سه‌گانه ذخیره، پردازش و توزیع داده پیام‌های شخصی در ماده ۵۹ قانون تجارت الکترونیکی جرم انگاری شده که تحلیل آن به شرح زیر است:

۲. ۲. ۱. ذخیره

ذخیره داده(Data Saving) به معنای اقدامی است که جهت نگهداری و حفاظت از داده و با ابزارهای مخصوص دارای حافظه انجام می‌گیرد. در مورد ذخیره داده پیام‌های شخصی حساس، پرونده شرکت فرانسوی SKF نمونه جالبی است. این شرکت بدون اطلاع به کمیسیون ملی اطلاعات و آزادی‌های فرانسه، اطلاعاتی را در مورد زندگی خصوصی، عقاید سیاسی متقاضیان کار و عضویت آنان در اتحادیه‌های کارگری در یک دستگاه دستی ذخیرهٔ داده‌ها نگهداری می‌کرد. این عمل نقض ماده ۴۲ قانون پردازش داده‌ها و آزادی‌های فردی ۱۹۸۷ محسوب می‌شد.[۱]

کمیسیون اطلاعات و آزادی‌ها پرونده را به دادستان کل ارسال کرد که خواستار جریمه‌ای معادل درآمد یک سال شرکت بود(زیبر، ۱۳۹۰: ۵۶) در بسیاری از موارد تطبیق حکم بر مصداق، کار دشواری است و تعیین این که آیا داده های ذخیره شده از سوی افراد دارای موقعیت‌های خاص نقض حقوق حمایت داده‌ها محسوب می‌شود یا نه، از اهمیت بالایی برخوردار است. به‌عنوان نمونه در پرونده دیگری در ایتالیا مطرح شد که یک شرکت چندملیتی با نصب دو سیستم کنترل به نام‌های «گزارشگر سطح خدمات» و «تسهیلات کنترل دسترسی به منابع» اقدام به کنترل از راه دور و نظارت بر فعالیت‌های کارگران می‌کرد که پس از شکایت اتحادیه‌های کارگری دادگاه شرکت نامبرده را به نقض ماده ۴ قانون کارگران محکوم نمود در حالی که شرکت مدعی بود سیستم‌ها را

---

۱. در خصوص تجدیدنظرخواهی آقای ش. فرزند ح. با وکالت آقای ب. نسبت به دادنامه شماره ۹۱۰۹۹۷۰۲۳۰۶۰۰۲۷۰ مورخ ۹۱/۸/۱۳ صادره از شعبه ۱۰۸۳ دادگاه عمومی تهران که متضمن محکومیت مشارٌالیه به یک سال حبس از حیث اتهام دسترسی و ذخیره غیرمجاز به محتویات ایمیل های حاوی وضعیت جسمانی شاکی بدوی و هک آن در جریان فروش اینترنتی یک دستگاه ریش تراش است؛ با نگرش در مجموعه اوراق و محتویات پرونده بالاخص گزارش مورخ ۹۰/۵/۲۴ معاونت مبارزه با جرائم پلیس فتا صفحه بیست و سوم پرونده، اقرار و اذعان تجدیدنظرخواه به ارتکاب بزه به شرح اوراق تحقیق مقدماتی صفحات سی و سوم و سی و پنجم پرونده و صفحات سی و هفتم و سی و هشتم و هفتاد و سه پرونده نظر به اینکه از ناحیه وکیل تجدیدنظرخواه ایراد و اعتراض موجه و مدللی که موجبات نقض رأی صادره را فراهم آورد، به عمل نیامده و بر مبانی استدلال و استنباط دادگاه نخستین در احراز و تشخیص بزهکاری تجدیدنظرخواه و صدور حکم بر همین مبنا، خدشه و خللی مترتب نیست، لذا دادگاه ضمن رد تجدیدنظرخواهی عنوان شده، دادنامه معترضٌ‌عنه را با استناد به ماده ۲۵۷ قانون آیین دادرسی کیفری تأیید و استوار می‌نماید رأی صادره قطعی است.

رئیس شعبه ۳۸ دادگاه تجدیدنظر استان تهران ـ مستشار دادگاه

فقط برای محافظت از دارایی‌های خود و طراحی و مدیریت خودکار مورد استفاده قرار داده است(ماتسورا، ۲۰۰۲: ۲۳)

۲. ۲. ۲. پردازش

منظور از پردازش(Process)، هرگونه تحصیل، نگهداری، ساماندهی، ذخیره، حک و اصلاح، جایگزین کردن، استعمال، افشاء، انتقال، انتشار و اقدامات مشابه در خصوص داده‌ها است(نوری و نخجوانی، ۱۳۸۳: ۳۳) و در صورتی که عملیات ذخیره داده‌ها، اجرای عملیات منطقی- ریاضی نسبت به داده‌ها، تغییر، امحاء، بازآفرینی یا پخش داده‌ها با وسایل خودکار انجام یابد، پردازش خودکار داده‌ها نامیده می‌شود(همان:۶۰) در واقع پردازش داده‌ها است که به اشخاص و شرکت‌های تأمین کننده کالا و خدمات در فضای الکترونیکی امکان شناسایی، کشف، دسته‌بندی و اولویت‌بندی سلایق، خواسته‌ها و نیازهای مصرفی مشتریان را می‌دهد تا از این طریق تبلیغات متناسب و کالاها و خدماتی متناسب با علایق و خواسته‌های آنان ارائه نمایند.[۱]

۲. ۲. ۳. توزیع

توزیع(Distribution) داده‌ها به معنای پخش و ارسال داده‌های ذخیره یا پردازش شده و انتقال آن برای اشخاص و موسسات دیگر است که اغلب با مقاصد تجاری و در راستای بازاریابی صورت می‌گیرد.[۲] چنانچه داده‌های موضوع جرم در قالب صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا

---

۱. در یکی از آراء شعبه ۱۰۱ دادگاه کیفری قم آمده است: « در رابطه با اتهام آقای ع. م متولد: ۱۳۵۴ اهل و ساکن قم دایر بر فروش اطلاعات مسافران تورهای خارجی از طریق سامانه های رایانه ای با توجه به محتویات پرونده، شکایت شکات، گزارش مرجع انتظامی پلیس فتا و تحقیقات به عمل آمده منجر به صدور کیفرخواست از سوی دادسرای عمومی و انقلاب قم، نحوه اظهارات و اقاریر متهم در مرجع انتظامی دادسرا و دادگاه حاکی از آن است که متهم مدیر یک شرکت مسافربری بوده که پس از ورشکستگی و انحلال شرکت، اطلاعات مربوط به مسافران و مقاصد آنها و نوع هتل و امکانات انتخاب شده در سفرهای خارجی را از طریق سامانه های رایانه ای به شرکت مسافربری .... متعلق به آقای ج.ف. فروخته است...

فلذا بزه انتسابی محرز و مسلم تشخیص داده شد و موضوع منطبق با ماده ۵۹ قانون تجارت الکترونیکی می باشد و دادگاه با استناد به ماده مذکور متهم موصوف را به تحمل یک سال حبس تعلیقی محکوم می نماید...» رییس شعبه ۱۰۱ دادگاه عمومی جزایی قم

۲. برابر بخش هایی از دادنامه شماره: ۹۱۰۹۹۷۲۱۹۱۴۰۱۱۰۳ شعبه ۱۰۳۹ دادگاه کیفری دو تهران: «به موجب کیفرخواست تقدیمی از دادسرای عمومی و انقلاب تهران خانم م.ص. فرزند یحیی، ۳۲ ساله، بیکار، باسواد، مجرد، متهم است به توزیع اطلاعات پرونده بیماران آقای ن.ر. متخصص اورولوژی و بیماری های جنسی و ارسال آن برای آقای س.ک. بدین توضیح که حسب شکایت شاکی و تحقیقات و گزارش پلیس فتا فاتب متهمه که منشی مطب شاکی بوده با دسترسی به اطلاعات پرونده های بیماران و تشخیص نوع بیماری و تفکیک و ذخیره سازی آن در یک فایل جداگانه، از طریق سامانه رایانه ای (اینترنت) مبادرت به انتقال شماره تماس، ایمیل و نوع بیماری افراد مورد نظر به آقای س.ک.

اسرار دیگری باشد، توزیع غیرقانونی آن مشمول ماده ۱۷ قانون جرایم رایانه ای است که برابر آن، هر کس به وسیله 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 دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از ۹۱ روز تا ۲ سال یا جزای نقدی از ۵ تا ۴۰ میلیون ریال یا هر دو مجازات محکوم خواهدشد.

یکی دیگر از نواقص قانونی در حمایت از داده‌های شخصی در قانون تجارت الکترونیکی، در مورد رفتارهای مجرمانه است. مقنن تنها رفتارهای سه گانه بالا را جرم انگاری کرده در حالی که «گردآوری» غیرمجاز داده پیام های شخصی که مهمتر از رفتارهای سه گانه دیگر است را جرم‌انگاری نکرده و هیچ یک از رفتارهای سه‌گانه نیز مترادف گردآوری داده‌ها نیست در نتیجه در حقوق ایران گردآوری غیرمجاز داده‌ها و به تبع آن سایر تکالیف پردازشگر در این خصوص ممنوع نبوده و مشمول حمایت کیفری نمی‌گردد(محسنی، ۱۳۸۹: ۵۷۰). خوشبختانه در ماده ۲۹ پیش نویس لایحه حمایت از داده‌ها، جمع‌آوری داده -به معنای گردآوری داده‌هایی که قبلاً ایجاد شده (بند ۴ ماده ۱ پیش نویس لایحه)- به صورت غیرمجاز را جرم انگاری کرده و خلأ قانون تجارت الکترونیک را پوشش داده است.

۲. ۳. شرایط و اوضاع و احوال

۲. ۳. ۱. رضایت شخص موضوع داده پیام

مطلق ذخیره، پردازش یا توزیع داده پیام‌های شخصی به معنای وقوع جرم ماده ۵۸ نیست، بلکه انجام این اعمال با قید «بدون رضایت صریح» اشخاصی که داده پیام‌ها مربوط به اوست، محقق کننده جرم است. پس اگر شخصی که داده پیام‌ها مربوط به اوست صریحاً رضایت خود را اعلام کرده باشد، جرم مورد نظر واقع نمی‌شود.

نموده است و متهم ردیف دوم هم اقدام به برقراری ارتباط ایمیلی و پیامکی و معرفی محصولات ویژه آقایان می کرده که با گلایه چند نفر از بیماران به دکتر متخصص و اعلام پزشک به پلیس فتا و پیگیری آن، قضیه کشف شده است.

دادگاه با بررسی اوراق پرونده، ملاحظه شکایت شاکی و مستندات ابرازی ایشان و نظریه مقرون به واقع متهم در مرحله تحقیقات مقدماتی هر چند در مرحله دادرسی منکر اقدام ارتکابی شده است و نظر به اینکه حسب پاسخ پلیس فضای تولید و تبادل اطلاعات انتقال از طریق ip متعلق به متهمه انجام گرفته است و سایر قراین و امارات موجود در پرونده، دادگاه اقدام مرتکب را مصداق بزه ماده ۵۹ قانون تجارت الکترونیکی دانسته و متهمه را به یک سال حبس با احتساب ایام بازداشت قبلی محکوم و اعلام می دارد رای صادره حضوری و ظرف مهلت بیست روز پس از ابلاغ قابل تجدیدنظرخواهی در دادگاه تجدیدنظر مرکز استان تهران می باشد.»

مقنن رضایت را مقید به قید «صریح» کرده بدون اینکه مفهوم آن را بیان و شیوه خاصی را برای کشف رضایت صریح تعیین کند. از حیث مفهومی، مراد از رضایت صریح، هرگونه ابراز و اظهار آگاهانه و از روی اختیار است که دلالت بر موافقت داشته باشد. این نشانه دال بر موافقت، نیازمند نوع اقدام عملی از شخص موضوع داده‌ها است و بنگاه الکترونیکی نمی‌تواند رضایت به پردازش داده‌های حساس را از سکوت و عدم اقدام استنباط کند. رضایت صریح شامل امری کاملاً واضح است و جزئیات معین مربوط به پردازش را در بر می‌گیرد و رضایت مبهم کفایت نمی‌کند.

۲. ۳. ۲. ساز و کار احراز رضایت

از حیث شیوه اطلاع از رضایت صریح، باید دانست رضایت چه در مورد داده‌های حساس و چه در خصوص داده‌های دیگر، اغلب با کلیک کردن به دست می‌آید. این امر، به معنای وجود یک صفحه ثبت نام در وب سایت است که در آن، شخص موضوع داده‌ها، پس از تکمیل اطلاعات خواسته شده، بر روی نماد «قبول می‌کنم» کلیک می‌کند. به این ترتیب این امر تضمین می‌شود که شرایط حمایت از داده‌ها، به اطلاع شخص رسیده و از بازدید کننده خواسته شده که رضایت خود را به‌صورت عملی اعلام کند(نوری و نخجوانی، ۱۳۸۳: ۹۱)

متأسفانه در پیش‌نویس لایحه نیز هر چند برابر بند ۳-۱- ماده ۱۵ از جمله موارد مجاز ایجاد و پردازش داده‌های شخصی حساس جایی است که «شخص موضوع داده رضایت صریح خود را به این امور بیان کرده باشد»، با وجود این، سازوکار مطمئنی برای احراز رضایت تعیین نکرده است. به نظر می‌رسد پیش بینی سازوکاری مشابه آنچه در ماده ۱۰ پیش نویس لایحه «مدیریت پیام‌های ناخواسته الکترونیکی» مصوب ۱۳۸۷ آمده می‌تواند تضمین کننده اطمینان از وجود رضایت شخص موضوع داده پیام‌ها باشد. برابر ماده مذکور: «تبلیغ باید با رضایت صریح دریافت کننده باشد. تبلیغ کننده موظف است در اولین پیام تبلیغاتی الکترونیکی خود که برای اخذ رضایت صریح ارسال می‌کند با توجه به ویژگی‌های فنی و اجرایی هر یک از انواع سیستم‌های پیام‌رسان الکترونیکی داخلی، ضوابط ذیل را به شکل قابل درک برای دریافت‌کنندگان رعایت کند: درج برچسب تبلیغاتی به‌طور قابل فهم و مشخص در عنوان پیام؛ شرح موضوع تبلیغ؛ پیش‌نویس امکان انصراف کاربر جهت عدم دریافت مجدد پیام تبلیغاتی به شیوه ای آسان و بدون هزینه و قید و شرط؛ شرح دقیق نحوه دستیابی به ادرس و یا شماره تماس الکترونیکی و یا دیگر اطلاعاتی که منجر به ارسال پیام تبلیغاتی شده است؛ مدت زمان اعتبار رضایت کاربر.»

در انگلستان برابر قانون حمایت داده ها مصوب ۱۹۹۸ در صورتی که داده‌ها به‌طور مستقیم از شخص موضوع داده‌ها بدست نیامده باشد، کنترل کننده باید تا حد ممکن نسبت به آگاه بودن این

شخص از اطلاعات مربوط اطمینان حاصل کند. برابر ضمیمه دو این قانون، پردازش فقط در صورت تحقق یکی از شرایط زیر صورت خواهد گرفت:

۱. فرد، رضایت خود را مبنی بر پردازش اعلام کرده باشد؛
۲. پردازش در راستای اجرای قرارداد منعقد شده با شخص موضوع داده‌ها، ضروری باشد؛
۳. پردازش بر طبق تکلیف قانونی الزامی باشد؛
۴. پردازش در جهت حمایت از منافع حیاتی شخص ضروری باشد؛
۵. پردازش برای انجام وظایف عمومی ضروری باشد؛
۶. پردازش جهت پیگیری منافع مشروع تاجر ضروری بوده و برای منافع شخص موضوع داده‌ها هم زیان‌آور نباشد(چسیک، ۲۰۰۲: ۲۱۵).

۲. ۳. ۳. شرایط تکمیلی رضایت

در مورد شرط رضایت باید دانست که اول: رضایت فرد تنها در محدوده اجازه صریح وی معتبر است و تجاوز از محدوده مجاز به منزله عدم رضایت است؛ دوم: رضایت تحت حکومت عفت عمومی و اخلاق حسنه و عرف جامعه است چرا که ممکن است اشخاصی باشند که هیچ حریمی برای خود نشناسند و اعمال آنان مشمول عناوینی چون اشاعه فحشاء باشد. از این روی رضایت، مجوز تام پردازش داده‌های شخصی نیست. ماده ۵۹ ق.ت.ا. که در فصل مربوط به حمایت از داده پیام‌های شخصی و بعد از ماده ۵۸ ذکر شده، مقرر نموده است: «در صورت رضایت شخص موضوع داده پیام نیز به شرط آن‌که محتوای داده پیام وفق قوانین مصوب مجلس شورای اسلامی باشد، ذخیره پردازش و توزیع داده پیام‌های شخصی در بستر مبادلات الکترونیکی باید با لحاظ شرایط زیر باشد:...».

۲. ۳. ۳. ۱. موافقت با قوانین موضوعه: این شرط با عبارت «به شرط آن‌که محتوای داده پیام وفق قوانین مصوب مجلس شورای اسلامی باشد» مذکور در ماده ۵۹ بیان شده و مراد از آن این است که صرف رضایت صاحب داده پیام شخصی، مجوز ذخیره، پردازش یا توزیع آن نیست بلکه افزون بر آن محتوای داده باید به‌گونه‌ای باشد که ذخیره، پردازش یا توزیع آن از نظر قانونی منعی نداشته باشد. برابر منطوق ماده ۵۹ ق.ت.ا.، تنها مطابقت با قوانین «مجلس شورای اسلامی» شرط شده است و در چارچوب تفسیر لفظی و مضیّق قوانین کیفری که مستظهر به اصل اباحه است، چنانچه ذخیره پردازش و توزیع داده پیام‌های شخصی با قوانین مصوب مجلس مغایرت نداشته باشد، منعی ندارد. این تفسیر هر چند در راستای تفسیر به نفع متهم است، لکن دیدگاه مبتنی بر تفسیر منطقی آن است که تصریح به «قوانین مصوب مجلس شورای اسلامی»، به جهت جنبه غالبی قوانین است که مصوب مجلس هستند و گرنه، ذخیره، پردازش یا توزیع داده پیام به وجه مغایر با

قوانین وضع شده از سایر مراجع ذی‌صلاح - مانند مجمع تشخیص مصلحت– نیز امکان پذیر نخواهد بود، به‌ویژه که صلاحیت تقنینی مجمع تشخیص مصلحت نظام علی القاعده در مقام حل اختلاف بین مجلس و شورای نگهبان است و این بدان معنا است که در نظام قانونگذاری ایران، مرجع بالاتر به شمار می آید.

۲. ۳. ۳. ۲. تشریح اهداف ذخیره، پردازش یا توزیع داده پیام‌های شخصی: متن ماده ۵۹ ق.ت.ا. با تصریح به شرایط بالا، اعلام کرده که ذخیره، پردازش و توزیع داده پیام‌های شخصی باید با لحاظ شرایط زیر صورت پذیرد که بند الف آن مقرر می‌دارد: «اهداف آن مشخص بوده و به‌طور واضح شرح داده شده باشد.» بنابراین چنانچه هدف ذخیره، پردازش یا توزیع داده پیام شخصی مشخص نبوده و به‌صورت روشنی تشریح نشده باشد–حتی با وجود رضایت شخص موضوع داده پیام نیز–، جرم واقع شده است.

۲. ۳. ۳. ۳. عدم جمع‌آوری غیر ضروری یا استفاده خلاف هدف جمع‌آوری داده پیام‌های شخصی: بند ب ماده ۵۹ شرط دیگر وقوع جرم را بدین نحو اعلام کرده که: «داده پیام باید تنها به اندازه ضرورت و متناسب با اهدافی که در هنگام جمع‌آوری برای شخص موضوع داده پیام شرح داده شده جمع‌آوری گردد و تنها برای اهداف تعیین شده مورد استفاده قرار گیرد.» این بند خود از دو قسمت تشکیل شده است: اول: با توجه به اهدافی که در هنگام جمع‌آوری داده پیام‌ها برای شخص موضوع داده پیام تشریح شده –و آن هم صرفاً در حدی که برای آن هدف ضرورت دارد–، جمع‌آوری شود و جمع‌آوری اطلاعات غیر ضروری یا غیر از آنچه که به شخص گفته شده، جرم است؛ دوم: از همان اطلاعات جمع‌آوری شده نیز باید صرفاً در راستای همان اهدافی که تعیین شده استفاده شود و استفاده از داده پیام‌های جمع آوری شده با رضایت شخص بر خلاف آن اهداف، جرم است.

۲. ۳. ۳. ۴. ذخیره، پردازش یا توزیع داده پیام نادرست یا غیر روز آمد: این شرط در بند (ج) ماده ۵۹ بدین نحو بیان شده که: «داده پیام باید صحیح و روزآمد باشد.» بنابراین اگر اطلاعاتی نادرست که مثلاً در مورد عقاید شخص صدق نمی‌کند یا اطلاعاتی کهنه مثلاً مربوط به مذهب سابق وی جمع‌آوری شده باشد، جرم را محقق می‌نماید.

۲. ۳. ۳. ۵. امکان دسترسی شخص موضوع داده پیام به پرونده‌های رایانه ای مربوط به خود: این شرط نیز در بند (د) ماده ۵۹ بدین شرح بیان شده که: «شخص موضوع داده پیام باید به پرونده‌های رایانه‌ای حاوی داده پیام‌های شخصی مربوط به خود دسترسی داشته و بتواند داده پیام‌های ناقص و یا نادرست را محو یا اصلاح کند.» بدیهی است امکان انجام این امور باید توسط شخص یا مرجعی که داده پیام‌های شخصی را ذخیره، پردازش یا توزیع می‌کند فراهم شود و این شخص یا مرجع باید اول: امکان دسترسی شخص موضوع داده پیام به پرونده‌های رایانه‌ای حاوی اطلاعات شخصی خود را

فراهم سازد و دوم: این امکان نیز فراهم باشد که بعد از دسترسی به پرونده رایانه‌ای امکان محو یا اصلاح داده پیام‌های ناقص توسط وی وجود داشته باشد.

۲. ۳. ۳. ۶. امکان محو کامل پرونده رایانه‌ای داده پیام‌ها شخص به درخواست شخص موضوع داده پیام: این شرط در بند (هـ) ماده ۵۹ بدین نحو بیان شده که: «شخص موضوع داده پیام باید بتواند در هر زمان با رعایت ضوابط مربوطه درخواست محو کامل پرونده رایانه‌ای داده پیام‌های شخصی مربوط به خود را بنماید.» مراد از این شرط آن است که شخص موضوع داده پیام در هر زمانی حق داشته باشد از ذخیرهٔ اطلاعات مربوط به خود منصرف شده و از شخص یا مرجعی که اطلاعات مربوط به وی را در اختیار دارد بخواهد که پرونده حاوی اطلاعات وی را محو نماید. این شرط بیانگر تأثیر رضایت شخص موضوع داده پیام در وقوع جرم است که همان‌گونه که در ابتدا حدوث رضایت وی امکان ذخیره، پردازش و توزیع داده پیام‌های شخصی مربوط به وی را تجویز می‌کند، استمرار این عمل نیز منوط به بقای رضایت اوست و در صورت عدم بقای رضایت، شخص یا مرجع مسئول باید درخواست وی مبنی بر محو کامل پرونده رایانه‌ای را پذیرفته، مورد بررسی قرار دهد و در صورتی که با ضوابط قانونی مغایرت نداشته باشد سریعاً پرونده رایانه‌ای حاوی اطلاعات شخصی درخواست کننده را محو نماید.

ایراد دیگر در مورد رفتار مجرمانه، عدم تعیین استثنائات ذخیره، پردازش و توزیع داده پیام های شخصی حساس است. توضیح اینکه هر چند در تعیین رفتارهای مجرمانه هر جرمی استثنائات آن بسیار مهم است، لکن در این زمینه قانون تجارت الکترونیکی تنها در ماده ۶۱ مقرر داشته: «سایر موارد راجع به دسترسی موضوع «داده‌پیام» از قبیل استثنائات، ... به موجب مواد مندرج در باب چهارم این قانون و آیین نامه مربوطه خواهد بود.» در حالی‌که جدا از عدم تصویب آیین‌نامه مربوطه، در مواد ۷۱ و ۷۲ و ۷۳ باب چهارم این قانون هم که ناظر به این موضوع است مقررات خاصی در این زمینه وجود ندارد! در این زمینه بند ۳ ماده ۱۵ پیش نویس لایحه حمایت از داده‌ها و حریم خصوصی در فضای مجازی موارد مجاز ایجاد یا پردازش یا استفاده از داده‌های شخصی حساس را تعیین کرده که به نظر می‌رسد باتوجه به عدم تعارض بین دو مقرره، در صورت قانونی شدن، بتوان با آن خلأ قانون تجارت الکترونیکی را پوشش داد.

۲. ۳. ۴. بستر وقوع جرم

شرط اساسی تحقق جرم نقض داده پیام‌های شخصی موضوع ماده ۵۸ ق.ت.ا.، وقوع رفتارهای مجرمانه در بستر تجارت الکترونیکی است. در مورد مفهوم تجارت الکترونیکی، تلاش‌های متعدد با نگاه‌های مختلف انجام یافته تا تعریفی از تجارت الکترونیکی ارائه گردد. در بخشی از سند راهبردی نظام جامع فناوری اطلاعات جمهوری اسلامی ایران مصوب هیات وزیران آمده است: «در ساده‌ترین تعریف می‌توان تجارت الکترونیکی را انجام امور تجارت بوسیله سامانه‌های الکترونیکی دانست. گروه مشاوره‌ای گارتنر به عنوان یک شرکت تحقیقاتی و مشاوره‌ای معتبر، تجارت الکترونیکی را میزان استفاده یک شرکت از

فرصتهای ایجادشده توسط شبکه اینترنت و فناوری‌های مرتبط معرفی نموده است. سازمان توسعه و همکاری‌های اقتصادی(OECD) نیز تجارت الکترونیک را انجام تجارت (خرید و فروش کالاها و خدمات) از طریق‌اینترنت، (خواه کالاها و خدماتی‌که قابلیت ارائه و تحویل از طریق اینترنت را دارند و خواه آنهایی که ندارند) خرید، فروش و مبادله کالا، خدمات و اطلاعات از طریق شبکه می‌داند.»(روزنامه رسمی، ۱۳۸۸: ش ۱۸۷۷۱)

طبق تعریف قانون اعتماد سازی در اقتصاد دیجیتالی فرانسه مصوب ۲۲ ژوئن ۲۰۰۴، تجارت الکترونیکی فعالیتی اقتصادی است که با بهره‌گیری از آن، شخص عرضه کالا یا خدمات از راه دور و از طریق الکترونیکی را پیشنهاد و تضمین می‌کند (دبلفون، ۱۳۸۸: ۲۵) به گفته بعضی، می توان گفت تجارت الکترونیک، ارتباطات تجاری بین اشخاص حقیقی و میان نهادهای تجاری را شامل می شود که در - یا بر روی - شبکه الکترونیک صورت می‌گیرند. این روابط می توانند شامل هر بخشی از روند تجاری باشند. موضوع این مطالعات می تواند اموال منقولی باشد که باید به صورت آنلاین تحویل داده شوند؛ مانند کتاب ها و دی وی دی ها برای تجارت الکترونیکی از نوع تولید– مصرف؛ و یا مواد شیمیایی در تجارت الکترونیکی از نوع تولید– تولید؛ و یا می توانند اموال غیر مادی باشند، مانند داده ها و اطلاعاتی که ممکن است به‌صورت آن لاین و یا آف لاین تحویل داده شود.(رید و انگل، ۲۰۰۷: ۱۹۸)

ایرادی که در مورد شرط وقوع جرم در بستر تجارت الکترونیکی وارد است اینکه باتوجه به فقدان تعریف قانونی از تجارت الکترونیکی و برداشت‌های مختلف از این اصطلاح، معلوم نیست که آیا طبق تعاریف متداول، این قانون شامل زیرشاخه‌های تجارت الکترونیکی نظیر بانکداری الکترونیکی، پزشکی الکترونیکی و غیره می شود یا اینکه برای هر کدام از این شاخه‌ها باید قانون جداگانه ای مشابه همین قانون وضع و تصویب کرد؟(محسنی، ۱۳۸۹: ۵۶۹) بالاتر از این حتی معلوم نیست که دامنه جرم محدود به تجارت الکترونیکی خالص است یا اینکه تجارت الکترونیکی بینابین را هم در بر می گیرد.

توضیح آنکه تجارت الکترونیکی سه بخش دارد: محصول، فرآیند و بازیگران تجارت؛ که ماهیت این سه بخش بر روی یک طیف از کاملاً فیزیکی تا کاملاً دیجیتالی قرار دارد. چنانچه ماهیت این سه بخش کاملا فیزیکی باشد، تجارت سنتی؛ اگر کاملا دیجیتالی باشد، تجارت الکترونیکی و اگر ماهیت این سه بخش حالت بینابین داشته باشد، تجارت نیمه الکترونیکی نامیده می‌شود(توربان، ۲۰۰۲: ۳۳). حال معلوم نیست که مراد از بستر تجارت الکترونیکی مورد نظر قانون تجارت الکترونیکی تنها نوع اول است یا اینکه نوع دوم را هم در بر می گیرد؟ ضمن اینکه طبق هر برداشتی از مفهوم تجارت الکترونیکی، نهایتاً دامنه جرم محدود به تجارت الکترونیکی است و گردآوری، ذخیره، پردازش و توزیع داده پیام های شخصی حساس در خارج از این قلمرو را در بر نمی گیرد.

این در حالی است که ماده ۵۸ ق.ت.ا. با اینکه ذیل مبحث اول از باب سوم این قانون با عنوان «حمایت انحصاری در بستر مبادلات الکترونیکی» قرار دارد، لکن ظاهر متن ماده مطلق بوده و دلالت بر ایجاد یک حکم عام دارد!!

۲. ۳. ۵. نتیجه جرم

از حیث نتیجه این جرم مطلق است و ذخیره، پردازش یا توزیع داده پیام‌های شخصی صرف نظر از ورود یا عدم ورود خسارت به شخص موضوع داده‌ها و یا کسب منفعتی برای متهم، جرم را محقق می‌سازد. مطلق بودن جرم به معنای عدم امکان تحقق شروع به جرم نیست. در این گونه جرایم شروع به جرم زمانی محقق می‌شود که متهم به قصد ارتکاب جرم شروع به انجام رفتارهای مادی جرم می کند، لکن به واسطه عوامل خارج از اداره او قصدش معلق می ماند.(ماده ۱۲۲ ق.م.ا.)

اما در بخشی از ماده ۲۹ پیش نویس لایحه حمایت از داده‌ها و حریم خصوصی در فضای مجازی آمده: «در صورتی‌که مرتکب این اقدامات را به قصد انتفاع مالی خود یا دیگری انجام داده باشد یا از این طریق موجب وارد شدن ضرر مالی یا حیثیتی به دیگری شده باشد...» با توجه به واژه «یا» که برای تفکیک دو فرض بکار رفته ظاهر ماده این است که مجازات ناظر به یکی از این دو صورت است و هر کدام به تنهایی مستوجب اعمال مجازات‌اند: «مرتکب این اقدامات را به قصد انتفاع مالی خود یا دیگری انجام داده باشد»؛ یا اینکه: «از این طریق موجب وارد شدن ضرر مالی یا حیثیتی به دیگری شده باشد » با چنین برداشتی جرم از حیث نتیجه هم فرض مطلق دارد و هم مقید! چون در فرض اول با صرف وجود سوء نیت خاص (قصد انتفاع مالی)، جدای از ورود یا عدم ورود خسارت، جرم قابل تحقق است. همچنین جرم از حیث سوء نیت خاص هم فرض مطلق دارد و هم مقید! چون در فرض دوم با صرف تحقق نتیجه (ضرر مالی یا حیثیتی)، جدای از وجود یا فقدان قصد انتفاع متهم، جرم قابل تحقق است. تبصره ۲ این ماده نیز مؤید این برداشت است که به موجب آن: «در مواردی که ایراد ضرر مالی یا حیثیتی ناشی از تقصیر مرتکب باشد... محکوم خواهد شد» این تبصره نشان می‌دهد که ایراد ضرر بدون وجود سوء نیت نیز، جرم را محقق می‌سازد.

۳. رکن معنوی

جرم مندرج در ماده ۵۸ ق.ت.ا. جرمی عمدی است و رکن معنوی جرایم عمدی از علم و عمد تشکیل شده است. بنابراین، مرتکب در صورتی مجرم شناخته می شود که اولاً بداند اطلاعات مربوط به یک شخص حقیقی مشخص و در زمره داده پیام های شخصی حساس است و ثانیاً با عمد و اراده خود داده‌های شخصی را ذخیره، پردازش و توزیع کرده باشد. از آنجا که جرم موضوع این ماده مطلق است و با صرف انجام عمدی این رفتارها محقق می‌شود، بنابراین نیازی به اثبات سوء نیت خاص متهم وجود ندارد. اما در خصوص رضایت یا عدم رضایت شخص موضوع داده پیام در ذخیره، پردازش یا توزیع آن،

اصل بر عدم رضایت اشخاص است و چنانچه متهم مدعی رضایت شخص موضوع داده پیام باشد، باید آن را اثبات کند.

جرم موضوع ماده ۵۹ این قانون نیز جرمی عمدی است و برای محکومیت متهم به ارتکاب جرم باید علم وی به موضوع و عمد وی در ذخیره، پردازش و توزیع داده پیام‌های شخصی و عدم رعایت شرایط مورد نظر احراز گردد. تنها در ماده ۷۳ ق.ت.ا. در مورد دفاتر خدمات صدور گواهی الکترونیکی، ارتکاب غیر عمدی این جرایم نیز پیش‌بینی شده است. دلیل این‌که ارتکاب عمدی جرایم راجع به داده پیام‌های شخصی توسط دفاتر خدمات صدور گواهی الکترونیکی مستوجب حداکثر مجازات است و نیز دلیل اینکه ارتکاب غیر عمدی جرایم توسط این دفاتر جرم انگاری شده، آن است که دفاتر مذکور از یک سوی امین تعداد زیادی از افراد به حساب می‌آیند و اطلاعات شخصی بسیاری از مردم را در اختیار دارند و از سوی دیگر اشخاص فعال در این دفاتر، افرادی آموزش دیده هستند و بی‌مبالاتی و بی‌احتیاطی آنان قابل تحمل نیست. با وجود این، در پیش نویس لایحه ایجاد، پردازش و استفاده غیرعمدی از داده‌های شخصی هم جرم انگاری شده و برابر تبصره ۲ ماده ۱۵ لایحه: «در مواردی که ایراد ضرر مالی یا حیثیتی ناشی از تقصیر مرتکب باشد، چنانچه داده‌های شخصی، حساس نباشد مرتکب به حداقل مجازات مقرر و چنانچه داده های شخصی، حساس باشند، به حداکثر مجازات محکوم خواهد شد».

۴. مجازات

۴. ۱. درجه جرم و آثار مترتب بر این درجه

مجازات جرم تعرض به داده پیام‌های شخصی حساس در ماده ۷۱ ق.ت.ا. یک تا سه سال حبس تعیین شده است. مجازات جرم ماده ۷۱ ق.ت.ا. درجه پنج به شمار می‌آید در حالیکه در ماده ۲۹ پیش نویس لایحه این جرم مستوجب حبس یا جزای نقدی درجه ۶ و مجازات جرم موضوع ماده ۶۸ پیش‌نویس لایحه «صیانت و حفاظت از داده‌های شخصی» حسب مورد درجه شش یا پنج است. تفاوت این مجازات‌ها در آثار محکومیت و اعمال سازوکارهای ارفاقی است. به عنوان نمونه شروع به جرم درجه پنج مجازات دارد ولی شروع به جرم درجه شش مجازات ندارد(ماده ۱۲۲ ق.م.ا.)؛ مرور زمان تعقیب و مجازات جرم درجه پنج، به ترتیب هفت سال و ده سال ولی در جرم درجه شش، پنج سال و هفت سال است(مواد ۱۰۵ و ۱۰۷ ق.م.ا.)؛ جرم درجه پنج مشمول تعویق صدور حکم نمی‌شود ولی صدور حکم جرم درجه شش قابل تعویق است(ماده ۴۰ ق.م.ا.)؛ در جرم درجه شش توبه متهم موجب سقوط مجازات و در جرم درجه پنج موجب تخفیف مجازات است(ماده ۱۱۵ ق.م.ا.)؛ در جرم درجه شش تعلیق تعقیب و میانجیگری امکان دارد ولی در جرم درجه پنج امکان ندارد(ماده ۸۰ و۸۲ ق.آ.د.ک.)

۴. ۲. مجازات تعدد و تکرار جرم

در صورت تعدد جرایم ناقض داده پیام‌های شخصی حساس، اگر جرایم ارتکابی دو یا سه فقره باشد، حداکثر مجازات(سه سال حبس) حکم داده می‌شود و اگر جرایم ارتکابی بیش از سه فقره باشد، مجازات مرتکب، از بیش از حداکثر تا یک و نیم برابر (سه سال و یکروز تا چهار سال و نیم) خواهد بود.

همچنین در صورت تحقق وضعیت تکرار جرم(داشتن سابقه محکومیت کیفری به جرم تعزیری درجه یک تا شش و وقوع جرم تعرض به داده پیام‌های شخصی حساس تا پیش از حصول اعاده حیثیت یا مرور زمان مجازات)، مجازات مرتکب، از بیش از حداکثر تا یک و نیم برابر (سه سال و یکروز تا چهار سال و نیم) خواهد بود.

۴. ۳. شرکت و معاونت در جرم

علی القاعده برابر ماده ۱۲۵ قانون مجازات، مجازات شریک جرم، مجازات فاعل مستقل آن جرم است. پس اگر الف و ب با مشارکت هم اقدام به ذخیره یا پردازش داده پیام شخصی حساس متعلق به ج کنند، هر یک از الف و ب مستقلاً به یک تا سه سال حبس محکوم می‌شوند. همچنین در صورتی که شخص الف داده پیام را ذخیره، ب آن را پردازش و ج آن را توزیع نماید و شخص د در هر سه فعل شریک باشد، الف، ب و ج هر کدام جداگانه به یک تا سه سال حبس محکوم می‌شوند و د که در سه جرم شرکت کرده، از باب تعدد جرم به حداکثر مجازات یعنی سه سال حبس محکوم می‌شود.

همچنین چون این جرم درجه پنج به شمار می‌آید اگر کسی مباشر جرم را تحریک و تشویق کند یا جرم را تسهیل کند، معاون جرم به شمار آمده و مجازات معاون برابر مقررات ماده ۱۲۷ ق.م.ا. یک تا دو درجه کمتر از مباشر جرم است که ممکن است مجازات زندان درجه شش یا هفت و یا مجازات درجه شش یا هفت از نوع دیگر مانند جزای نقدی باشد.

از سوی دیگر، برابر ماده ۶۹ « لایحه صیانت و حفاظت از داده‌های شخصی» در صورت وجود یک یا چند شرط ذیل، مجازات مرتکب یک یا دو درجه بالاتر تعیین می‌شود: الف)به‌واسطه شغل یا حرفه خود مرتکب جرم شده باشد؛ ب)نسبت به گستره و دامنه فعالیت خود، شمار قابل‌توجهی از اشخاص را هدف قرار داده باشد؛ پ)زیان مادی یا آسیب معنوی قابل‌توجه یا جبران‌ناپذیری را وارد آورده باشد؛ ت)داده‌های شخصی حیاتی یا حساس، ابزار یا نتیجه جرم باشند؛ و ث)به شکل گروهی یا سازمان‌یافته مرتکب شده باشد. در این موارد مجازات مرتکب حسب مورد درجه سه وچهار نیز خواهد بود که در این صورت در آثاری همچون امکان یا عدم امکان تعلیق مجازات(ماده ۴۶ ق.م.ا.)، نظام نیمه آزادی(ماده ۵۷ ق.م.ا.)، نظارت الکترونیکی(ماده ۶۲ ق.م.ا.)، صلاحیت دادگاه کیفری(ماده ۳۰۲ ق. آ.د.ک.) و ... متفاوت خواهند بود.

اینها و تفاوت‌های بسیار دیگر نشاندهنده اهمیت تشخیص قانون حاکم و تعیین درجه جرم است که در ادامه بررسی می‌شود.

نتیجه‌گیری

هر چند جرم انگاری و حمایت کیفری از داده پیام‌های شخصی در تجارت الکترونیکی امری ضروری و لازمه جلب اعتماد مصرف کنندگان و ترغیب به انجام خرید و فروش الکترونیکی است، اما وضع ماده ۵۸ و ۵۹ قانون تجارت الکترونیکی و ضمانت اجرای آن در ماده ۷۱ این قانون، با چالش های درون متنی و برون متنی روبرو است.

در بعد درون متنی، نقص قانون ناشی از انحصار حمایت قانونی به «داده پیام‌های شخصی حساس» و عدم حمایت قانونی از سایر «داده پیام‌های شخصی» داخل در قلمرو حریم خصوصی افراد و نیز جرم انگاری نکردن سایر روش‌های نقض داده پیام‌های شخصی است؛ اجمال قانونی ناشی از عدم ارائه تعریف از تجارت الکترونیکی و تردید در شمول دامنه جرم نسبت به همه یا بعضی از اقسام تجارت الکترونیکی است. ابهام قانونی همچنین ناشی از عدم صراحت، تفسیرپذیری و امکان برداشت‌های مختلف از واژه‌های بکار رفته در متن قانون -به ویژه واژه‌های تبیین کننده داده پیام‌های شخصی حساس- است.

اما از بعد برون متنی، چالش قانون ناشی از رابطه قانون تجارت الکترونیکی با سایر قوانین موضوعه مانند قانون مجازات اسلامی ۱۳۹۲، قانون آیین دادرسی کیفری ۱۳۹۲، پیش نویس «لایحه حمایت از داده و حریم خصوصی در فضای مجازی» دی ماه ۱۳۹۶ و پیش‌نویس لایحه «صیانت و حفاظت از داده‌های شخصی» است که در تیرماه ۱۳۹۷ از سوی وزارت ارتباطات و فناوری اطلاعات تهیه و منتشر شده است.

قلمرو اجرای این لایحه حمایت، فضای مجازی و قلمرو اجرای لایحه صیانت، عام و کلی است و از آنجا که دامنه شمول قانون تجارت الکترونیکی، بستر مبادلات الکترونیکی است، پرسش این است که در صورت قانون شدن لایحه، در موارد خلأ قانونی یا تعارض، رابطه این دو چگونه خواهد بود؟

هر چند در ادبیات حقوقی به یک قاعده اصولی استناد می شود که «عام مؤخّر، ناسخ خاص مقدم نیست»[1] و بر این پایه باید گفت در موارد تعارض بین قانون تجارت الکترونیکی، {قانون} حمایت از

---

۱. بخشی از اظهارات دادستان کل کشور هنگام صدور رأی وحدت رویه شماره ۶۶۴-۱۳۸۲/۱۰/۳۰ : « با فرض تعارض بین مقررات مندرج در بند ۵ ماده ۵ قانون تشکیل دادگاههای عمومی و انقلاب مصوب ۱۳۷۳ با تبصره ذیل ماده ۴ این قانون اصلاحی ۱۳۸۱، موضوع مشمول قاعده تعارض بین عام موخر با خاص مقدم می باشد که قطع نظر از آراء بسیاری از فقها و اصولیین که قایل به تخصیص حکم عام موخر با خاص مقدم می باشند، هیأت محترم عمومی دیوان عالی کشور بموجب آرای متعددی از جمله رأی وحدت رویه شماره: ۲۱۲ منتشره در مورخ ۱۳۵۰/۸/۶ که نسبت به عدم

داده‌ها و حریم خصوصی در فضای مجازی و {قانون} «صیانت و حفاظت از داده‌های شخصی»، مقررات قانون تجارت الکترونیکی به اعتبار خود باقی است، اما از دید نگارنده گرچه این قاعده اصولی بین اصولیین مشهور است(مظفر، ۱۳۸۰: ۱۷۹؛ خراسانی، ۱۳۸۴، ج۲: ۱۹۲؛ مکارم شیرازی، ۱۳۸۲، ج ۲: ۱۵۷)، اما اول: در این مورد بین اصولیین اختلاف نظر وجود دارد و گروهی مثل شیخ طوسی و سید مرتضی و سید ابن زهره معتقدند که عام بعدی ناسخ خاص خواهد بود. قول سومی نیز وجود دارد و آن قول به توقف و رجوع به مرجحات است. بر اساس این عقیده اگر مرجحات خارجی وجود داشته باشد باید حکم عام را ناسخ قرار داد و الا حکم خاص، مخصص عام خواهد بود.(محمدی، ۱۳۹۶: ۱۰۹)؛ دوم: به فرض پذیرش این قاعده در اصول فقه، در حقوق موضوعه عرفی زمانی کاربرد دارد که قرینه‌ای دال بر تغییر منظور قانونگذار نباشد وگرنه، قانونّ عامّ مقدم حاکم خواهد بود. این برداشت مبتنی بر روش تفسیر غایی منتهی به کشف اراده واقعی قانون‌گذار است که با رویکرد تفسیر به نفع متهم نیز سازگاری دارد.

گفتنی است عدول از این قاعده در نظام حقوقی ما خیلی هم بیگانه نیست. به‌عنوان نمونه در مورد مقررات شروع به جرم، هر چند ق.م.ا. قانون عام است و طبق این قاعده باید مقررات شروع به جرم در قوانین خاص پیش از تصویب قانون مجازات به اعتبار خود باقی باشند، لکن همان گونه که در نظریه مشورتی شماره ۷/۹۲/۱۳۲۰ مورخ ۱۳۹۲/۷/۷ اداره کل حقوقی قوه قضائیه آمده، از آنجا که قانون‌گذار در مقام یکسان‌سازی و ایجاد نظم برای مجازات شروع به جرم بوده بنابراین باید قائل به نسخ حکم قوانین خاص مقدم و اجرای قانون عام مؤخر باشیم.

بنا بر آنچه گفته شد، در بحث جاری هم با توجه به تغییرات سریع فناوری ارتباطی و پیدایش روش‌های نوین نقض حریم خصوصی و داده‌های شخصی، لزوم بروز بودن مقررات حاکم بر فضای مجازی و اینکه لوایح جدید نشان‌دهنده آخرین خواست قانون‌گذار در زمینه تعرض به داده پیام‌های شخصی در فضای مجازی است، از این روی اولاً در موارد خلأ قانونیِ قانون تجارت الکترونیک -مانند عدم حمایت از داده پیام‌های شخصی یا اضرار ناشی از تقصیر مرتکب در تعرض به داده پیام‌های شخصی حساس- و ثانیاً در موارد تعارض قوانین -مانند میزان مجازات تعرض به داده پیام های حساس و آثار مترتب بر درجه جرم در قانون مجازات اسلامی و قانون آیین دادرسی کیفری- مقررات لایحه حمایت از داده‌ها و حریم خصوصی در فضای مجازی و در صورت تبدیل هر دو لایحه به قانون، در موارد خلأ یا تعارض بین لایحه حمایت از داده‌ها و حریم خصوصی در فضای مجازی و لایحه

شمول مقررات عام قانون مالیاتی مصوب سال: ۱۳۳۵ به مقررات خاص مالیاتی تجار ورشکسته موضوع قانون مصوب سال: ۱۳۱۸ اتخاذ تصمیم نموده است. همچنین بموجب رأی شماره: ۵۹/۲۹ مورخ: ۱۳۶۰/۱/۱۵ نسبت به عدم شمول مقررات عام قانون افراز و فروش املاک مشاع مصوب: ۱۳۷۵ به مقررات خاص شرکاء محجور موضوع قانون امور حبسی مصوب ۱۳۱۹ اعلام رأی نموده است لذا طبق رویه قضایی موجود حکم عام موخر ناسخ حکم خاص مقدم نمی باشد...»

«صیانت و حفاظت از داده‌های شخصی»، مقررات هر کدام از لوایح که از حیث تاریخ، پس از دیگری تصویب شود، باید اعمال شود و هر قانونی که دیرتر تصویب شود، ناسخ مقررات قانونی که پیشتر تصویب شده خواهد بود!

منابع

انصاری، باقر (۱۳۸۶)، **حقوق حریم خصوصی**، تهران: سازمان مطالعه و تدوین کتب علوم انسانی(سمت).

پلومان، ادوارد (۱۳۸۰)، **حقوق بین الملل ارتباطات و اطلاعات**، ترجمهٔ بهمن آقایی، چاپ اول، تهران: گنج دانش.

جعفری، علی (۱۳۹۶)، **ماهیت و مبانی حریم خصوصی اطلاعات**، تهران: پژوهشکده باقرالعلوم(ع).

جلالی فراهانی، امیر حسین (۱۳۸۹)، **کنوانسیون جرایم سایبر و پروتکل الحاقی آن**، تهران: انتشارات خرسندی.

حسن بن یوسف بن مطهر اسدی حلّی(۱۴۱۰ ه ق)، **إرشاد الأذهان إلی أحکام الإیمان**، قم: چاپ اول، ج۲، دفتر انتشارات اسلامی.

حیدری، علی مراد (۱۳۹۲)، «نقد کیفرشناختیِ تشهیر رسانه‌ای»، **حقوق اسلامی**، سال دهم، شماره ۳۸، ص ۱۶۰- ۱۳۳.

خرازی، محسن (۱۳۸۰)، «کاوشی در حکم فقهی تجسس»، **فقه اهل بیت**، سال هفتم، ش ۲۶، ص ۱۴۲- ۵۲.

خراسانی، محمدکاظم (۱۳۸۴)، **کفایه الاصول**، چاپ دوم، ج ۲، قم: موسسه النشر الاسلامی.

دبلفون، زویه لینان (۱۳۸۸)، **حقوق تجارت الکترونیک**، ترجمه و تحقیق ستار زرکلام، چاپ اول، تهران: شهر دانش.

دشتی، محمد (۱۳۹۰)، **ترجمهٔ نهج البلاغه حضرت امیرالمومنین علی(ع)**، چاپ اول، قم: انصارالمهدی.

زیبر، اولریش (۱۳۹۰)، **جرایم رایانه‌ای**، ترجمهٔ محمدعلی نوری و همکاران، چاپ دوم، تهران: کتابخانه گنج دانش.

السان، مصطفی (۱۳۹۱)، **حقوق تجارت الکترونیکی**، تهران: سازمان مطالعه و تدوین کتب علوم انسانی (سمت).

اداره کل قوانین (۱۳۸۵)، **طرح حمایت از حریم خصوصی**، دوره هفتم، سال سوم، ۱۳۸۵/۴/۸ شماره ثبت: ۵۶۰.

العاملی، زین‌الدین بن علی (۱۴۱۳ ه ق)، **مسالک الأفهام**، چاپ اول، ج ۹، قم: مؤسسهٔ المعارف الإسلامیهٔ.

کنیون، اندرو (۱۳۹۶)، **ابعاد جدید حقوق حریم خصوصی**، ترجمهٔ علی جعفری، تهران: پژوهشکده باقرالعلوم(ع).

محسنی، فرید (۱۳۸۹)، **حریم خصوصی اطلاعات**، مطالعه کیفری در حقوق ایران، ایالات متحده آمریکا و فقه امامیه، تهران: انتشارات دانشگاه امام صادق(ع).

محمدی، ابوالحسن (۱۳۹۶)، **مبانی استنباط حقوق اسلامی**، چاپ ۵۹، تهران: انتشارات دانشگاه تهران.

مظفر، محمدرضا (۱۳۸۰)، **اصول الفقه**، چاپ اول، قم: بوستان کتاب.

مکارم شیرازی، ناصر (۱۳۸۲)، **انوارالاصول**، چاپ دوم، ج۲، قم: مدرسه امام علی(ع).

مهرپور، حسین (۱۳۸۸)، **نظام بین‌المللی حقوق بشر**، تهران: انتشارات اطلاعات.

نوری، محمدعلی و نخجوانی، رضا (۱۳۸۳)، **حقوق حمایت داده‌ها**، چاپ اول، کتابخانه گنج دانش.

الهمیم، عبداللطیف (۲۰۰۳)، **الحیاه الخاصه فی‌الشریعه والقانون**، عمان، دار عمار.

Cohen, Julie E,(2000), **Informational Privacy and the Subject as Object**, Stanford Law Review, Vol.52,No.5.

European Data Protection Supervisor, Case Law Overview,(2016): https://edps.europa.eu/sites/edp/files/publication/17-04-27_annual_report_2016_en_1.pdf

Jeffrey Matsuura(2002), **Security, Rights and Liabilities in E.Commerce,** Artech House.

Llaudati, Arine, (2016), **Summaries of EU Court Decisions Relating to Data Protection** 2000-2015, European Anti Fraud Office.

Michael Chissick and Alistair Kelman(2002), **Electronic Commerce:** law and Practice, Sweet & Maxwell, London.

Turban, Efraim, King,David, Lee, Jae, Warkentin, Merrill, Chung, Michael, (2002), **Electronic Commerce**, Prentic Hall.

Walden, Ian(2007), **Computer Crime And Information Misuse**, Computer Law, Oxford University Press, Six Edition, Edited By: Chris Reed and John Angel.