

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

مأمّن حقوقی تجارت الکترونیک و جرائم رایانهای در ایران و سایر کشورها

مهندس محمدصادق معتمدی فر



وزارت فرهنگ و ارشاد اسلامی
مرکز توسعه فناوری اطلاعات و ارتباطات



سرشناسه

موحدی فر، محمدصادق، ۱۳۶۴ -

عنوان و نام پدیدآور

مسائل حقوقی تجارت الکترونیک و جرائم رایانه‌ای در ایران و سایر کشورها/ گردآوری محمدصادق موحدی فر.

مشخصات نشر

تهران: انتشارات آکادمیک، ۱۳۹۶.

مشخصات ظاهری

۵۵۰ ص: مصور، جدول.

شابک

۴۰۰۰۰۰ ریال 9-53-8423-600-978:

وضعیت فهرست‌نویسی: فیا

رده‌بندی کنگره

۵۶۴K: ۱۳۹۶ ۸ م ۲ ش/

رده‌بندی دیویی

۰۹۹۴۴/۳۴۳:

شماره کتابشناسی ملی: ۴۷۶۹۲۷۱



عنوان: مسائل حقوقی تجارت الکترونیک و جرائم رایانه‌ای در ایران و سایر کشورها

تألیف: محمدصادق موحدی فر

ویراستار: محسن نظر

انتشارات: آکادمیک

شابک: ۵۳-۸۴۲۳-۶۰۰-۶۰۰-۷۸

نوبت انتشار: ۱۳۹۶ - تهران

طراحی جلد: محمدعلی واعظی نژاد

قیمت: ۴۰۰۰۰ تومان

تیراژ: ۱۰۰۰ نسخه

چاپ و صحافی: دانشگاه خوارزمی

◀ فروشگاه مرکزی: خیابان قائم مقام، بالاتر از خ - مطهری، کوچه دهم، پلاک ۱۰، واحد ۱۰ - تلفن: ۸۸۵۳۶۷۳۶

◀ فروشگاه شماره ۲: خیابان مفتاح جنوبی، خ - خاقانی، دانشگاه خوارزمی - واحد انتشارات - تلفن: ۸۱۵۸۲۲۴۴

پست الکترونیکی: Academicpub1@gmail.com ■ وبسایت: Academicpress.co

Copyright

امروزه جایگاه فناوری اطلاعات در جوامع بشری بسیار گسترده شده است و بسیاری از جنبه‌های مختلف زندگی او را فراگرفته است. هر چه بیشتر زمان پیش می‌رود این موضوع ملموس‌تر از گذشته می‌گردد. در این اثنا یکی از مقولات مهم که رفاه و صرفه جویی در وقت و هزینه را به ارمغان آورده بحث زیبا و جذاب تجارت الکترونیک می‌باشد که دامنه وسیعی را شامل می‌شود. تجارت الکترونیکی مبتنی بر پردازش و انتقال الکترونیکی داده‌ها، شامل متن، صدا و تصویر می‌باشد. تجارت الکترونیکی فعالیت‌های گوناگونی از قبیل مبادله الکترونیکی کالاها و خدمات، تحویل فوری مطالب دیجیتال، انتقال الکترونیکی وجوه، مبادله الکترونیکی سهام، برنامه الکترونیکی، طرح‌های تجاری، طراحی و مهندسی مشترک، منبع یابی، خریدهای دولتی، بازاریابی، مستقیم و خدمات پس از فروش را از طریق شبکه‌های کامپیوتری و اینترنت در بر می‌گیرد. با توجه به اهمیت این موضوع باید به مسائل حقوقی و قانونی آن نیز توجه ویژه نمود.

Robert Dunne در کتاب کامپیوتر و قانون، قوانین و مسائل حقوقی آن را در سر فصل‌هایی مدون دسته بندی کرده که به شرح زیر می‌باشد:

- قوانین مدون و قوانین عمومی
- قراردادها
- شبه جرم
- توهین و تهمت
- شخص ثالث
- حق کپی رایت
- اسرار تجاری
- علامت تجاری
- حقوق حفظ حریم خصوصی
- پست الکترونیک

- حق تبلیغات
- قانون اساسی
- هرزگی و مسائل مربوط به منافی اخلاقی
- تبلیغات و پیام های ناخواسته

Anthony Reyes در کتاب تحقیقات جرایم سایبری می گوید: "هنوز جرایم اینترنتی از ایالتی با ایالت دیگر متفاوت می باشد." او همچنین روشهایی را جهت پیشگیری از وقوع جرایم و برخی از مسائل تکنیکی جهت نفوذ و ارتکاب جرم را بر می شمارد. **K. Jaishankar** صاحب کتاب جرم شناسی سایبری، برای فهم بهتر، مطالب را به بخشهای زیر جهت تحلیل سهلتر ارائه داده است:

- انحرافات و جرایم فرهنگی خرد در فضای مجازی
- دیدگاه مرموزان در مواجهه با استفاده از اینترنت
- سرقت مال دیجیتال
- جنایات سایبری
- مسائل حقوقی و سیاسی مربوط به جرایم سایبری

به گفته **David W. Brenner** قانون شکنی به دنبال درخواست منفعت بیشتر می آید. همچنین جرم و جنایت در مقوله های حقوق و مناطق جغرافیایی که در آن اجرای ضعیف است بیشتر ورود می کند.

ARNO R. LODDER, ANJA OSKAMP در کتاب فناوری اطلاعات و وکلا اذعان دارد که بین فناوری اطلاعات و قانون چنان ارتباطی وجود دارد که برای مردم نیز مبرهن است. می توان گفت ترکیب فناوری اطلاعات و وکلا یک ترکیب ذاتی بوده است که هم اکنون کشف شده.

برخی از سیاست گذاری ها مبتنی بر رفتارهای کاربران و نوع استفاده آنها از اینترنت می باشد که می توان از انواع وبکاوی و ردیابی رفتارها استفاده نمود و به وضع قوانین و برقراری سیاست درخور اقدام کرد.

بر مبنای نظر **Debra Littlejohn Shinder** نویسنده کتاب چشم اندازی از جرایم سایبری، این نوع جرایم بر اساس ۳ علت رخ می دهد: عوامل انسانی و عدم دانش کافی،

وجود راه نفوذ چه از دید سخت افزار و زیرساخت شبکه و چه از منظر نرم افزار ها و باز بودن حفره های امنیتی، سهل انگاری کاربران در حفظ و نگهداری مسائل امنیتی. جرایم سایبری در سه حوزه اصلی نماد پیدا کرده است: مسائل اقتصادی، اجتماعی و اخلاقی. در ایران عناوین جرایم رایانه ای به ۳۱ قسم تقسیم شده که شرح آن در ذیل ذکر شده است:

۱. دسترسی غیرمجاز به داده ها و سامانه های رایانه ای
۲. شنود غیرمجاز
۳. جاسوسی رایانه ای-دسترسی به داده های سری
۴. جاسوسی رایانه ای-دسترسی به داده های سری و قرار دادن در اختیار اشخاص فاقد صلاحیت
۵. جاسوسی رایانه ای-دسترسی به داده های سری و افشاء آنها برای دولتها و عوامل بیگانه
۶. نقض تدابیر امنیتی به قصد دسترسی به داده های سری
۷. سهل انگاری مأموران دولت منجر به جاسوسی
۸. جعل رایانه ای و استفاده از مجموع
۹. تخریب و اخلاف در داده ها
۱۰. از کار انداختن سامانه ها
۱۱. ممانعت از دسترسی
۱۲. تخریب و اخلاف در داده ها و از کار انداختن سامانه ها و ممانعت از دسترسی علیه سامانه های به کار رفته در خدمات عمومی با قصد به خطر انداختن امنیت مردم
۱۳. ربودن داده های دیگری با وجود عین داده در اختیار صاحب آن
۱۴. ربودن داده های دیگری بدون وجود عین داده در اختیار صاحب آن
۱۵. کلاهبرداری مرتبط با رایانه
۱۶. انتشار، توزیع یا معامله محتویات مستهجن یا نگهداری و تولید و ذخیره به انگیزه تجارت یا افساد

۱۷. انتشار، توزیع یا معامله محتویات مبتذل یا نگهداری و تولید و ذخیره به انگیزه تجارت یا افساد

۱۸. تحریک، ترغیب، تهدید یا تطمیع کند یا فریب افراد برای دسترسی به محتویات مستهجن یا تسهیل یا آموزش شیوه دسترسی

۱۹. محتویات مبتذل

۲۰. ارتکاب جرائم منافی عفت یا استعمال مواد مخدر یا خودکشی یا انحرافات جنسی یا اعمال خشونت‌آمیز

۲۱. متک حیثیت یا تغییر یا تحریف فیلم یا صوت یا تصویر دیگری و انتشار آن یا صرف انتشار علم به تغییر یا تحریف (تغییر و تحریف مستهجن حداکثر هردو مجازات)

۲۲. انتشار صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت

۲۳. نشر اکاذیب، فساد تشویش اذهان عمومی یا مقامات رسمی

۲۴. تولید یا انتشار یا ترویج اسلحه‌ها یا نرم‌افزارهایی که صرفاً برای ارتکاب جرم کاربرد دارند.

۲۵. فروش یا انتشار گذرواژه‌هایی که امکان دسترسی به داده یا سامانه‌های دیگری را فراهم کند

۲۶. انتشار یا در دسترس قرار دادن آموزش ارتکاب جرایم رایانه‌ای

۲۷. برقراری ارتباطات مخابراتی با استفاده از پهنای باند بین‌المللی از داخل به خارج از کشور و بالعکس

۲۸. عدم پالایش (فیلتر) محتوای مجرمانه از ناحیه ارائه‌دهندگان خدمات دسترسی مسترسی ناشی از عمد یا سهل انگاری

۲۹. خودداری از اجرای دستور حفاظت از داده‌ها یا افشاء داده‌های حفاظت شده یا آگاه نمودن اشخاصی که داده‌های مزبور به آنها مربوط می‌شود

۳۰. خودداری از اجرای دستور قضایی ارائه داده‌ها

پس از بررسی جرایم کامپیوتری، سایبری و اینترنتی می توان کمی در این حوزه خردتر و دقیق تر شد. دید حقوقی و قانونی صرفاً بر روی تجارت الکترونیکی که یکی از شاخه های مهم آن می باشد متمرکز گردد و موضوع بیشتر مورد بررسی و مطالعه قرار گیرد. با گسترش اینترنت فضای جدیدی برای وقوع جرایم بوجود آمده که از آن به جرایم اینترنتی یاد می شود همچون تدلیس در معامله الکترونیک، غش در معاملات الکترونیک، جرایم اخلاقی، اختلال در امنیت ملی و

در کتاب اینترنت و تجارت الکترونیک اثر **Peter Carey** مباحث مربوط به قوانین تجارت الکترونیک به بخش های ساختار جدید قرارداد، حقوق مالکیت فکری، حق انتشار، ثبت دامنه در فضای مجازی، حفاظت از داده ها، مقررات فروش دور، فناوری و اطلاعات مورد نیاز و قانون و صلاحیت تقسیم شده است.

یکی از مسائلی که در تجارت الکترونیک مطرح می شود بحث ثبت دامنه و محافظت از آن است و مسائل حقوقی و فنی که از آن مطرح می شود و موضوع فنی باید نخست مطرح گردد تا بتوان درباره آن نظر حقوقی اعلام نمود **Stephen Elias and Patricia Gima** در کتاب خود به بررسی انتخاب یک نام مالی، چگونگی محافظت از آن پرداخته است.

برای اخذ دامنه باید جهت ثبت به یک سرویس دهنده مراجعه کرده و آن را خریداری نمود. حال خود این موضوع اعم از نحوی خرید، نوع پرداخت، مبلغ، نوع و مفاد قرارداد فی مابین طرفین می تواند مسائلی را ایجاد کند که بار حقوقی خواهند داشت. از منظر جرم شناسی نیز می توان به آن نگاه کرد به عنوان مثال خرید یک دامنه در فاصله تمدید آن از طرف شخص ثالث که باعث آزرده گی مالک یا انواع سوء استفاده مالی شود یا از دید یک فرد متخصص، ثبت یک دامنه با عوض کردن نوع پسوند دات کام به دات ای آر که باعث بالا بردن نرخ رتبه بندی آن در موتورهای جستجو خواهد شد.

از نظر حفظ حق کپی رایت و ثبت حق اختراع در حوزه کامپیوتر¹ بایستی این امر پشـتوانه قانونی و حقوقی داشته باشد هنوز هم قوانین مربوطه در کشورهای مختلف شکلهای متنوع دارد.

برخی از مسائل مطروحه در حوزه تجارت الکترونیک که در دنیا و حتی کشور ایران مطرح است و موضوع مورد مطالعه و تحقیق می‌باشد به شرح ذیل آمده است:

- بررسی ابعاد حقوقی امضای الکترونیکی
- تحلیل شرایط اساسی تشکیل قرارداد در انعقاد قراردادهای الکترونیکی
- قابلیت استناد به ادله الکترونیکی
- ادول حاکم بر قانون تجارت الکترونیک ایران
- دادگاه صالح در حل اختلافات ناشی از قراردادهای الکترونیکی
- قانون حاکم در حل اختلافات ناشی از قراردادهای الکترونیکی
- حمایت از مصرف‌کننده در قراردادهای الکترونیکی با ارجاع دادگاه صالح و قانون حاکم
- آثار حقوقی تحقق اشتباه در انعقاد قراردادهای الکترونیکی
- زمان و مکان تشکیل قرارداد الکترونیکی
- وضعیت حقوقی نمایندگان الکترونیکی در انعقاد قراردادهای الکترونیکی
- آثار اشتباه نماینده الکترونیکی در انعقاد قراردادهای الکترونیکی
- مسئولیت واسطه‌ها در انعقاد قراردادهای الکترونیکی
- داوری الکترونیکی اختلافات
- تحلیل حقوقی شروط در قراردادهای الکترونیکی
- آثار حقوقی خطای وارداتی در مسیر انعقاد قراردادهای الکترونیکی
- مسئولیت غیر قراردادی در فضای مجازی
- نحوه تسلیم کالای دیجیتالی در بیع الکترونیکی

¹ Daniel Closal, Alex Gardinerl, Falk Giermsa, Jo "rg Machek, (2010). *Patent Law for Computer Scientists Steps to Protect Computer-Implemented Inventions*, Springer-Verlag Berlin Heidelberg

- نحوه اعمال اختیارات در بیع الکترونیکی
 - مسئولیت حقوقی ریشه (مرکز صدور گواهی امضای الکترونیکی)
 - قاجاق الکترونیکی کالا و ارز
 - بررسی شرایط تحقق سرقت حدی الکترونیکی
 - حمایت از داده‌های شخصی در فضای مجازی
 - نگاهی به جعل اسناد الکترونیکی
 - اعتبار حقوقی اسناد الکترونیکی
 - تحلیل قراردادهای خرید تجهیزات کامپیوتری
 - مسئولیت حقوقی واسطه‌های اینترنتی
 - تبعات حقوقی جاسوسی در فضای مجازی
 - اخلاق در فضای مجازی
 - قواعد حاکم بر تشکیل درآمدهای تجاری بین‌المللی در گستره ارتباطات نوین
 - حمایت از اسرار تجاری در گستره ارزش و تحلیل قواعد حاکم
 - قانون حاکم در اختلافات ناشی از تضییع حقوق مالکیت معنوی در گستره اینترنت
- طبق تبصره ۲۶ قانون دوم برنامه پنج ساله توسعه اقتصادی کشور (۱۳۷۸-۱۳۷۴)، وزارت بازرگانی موظف به ایجاد و راه‌اندازی تجارت الکترونیکی در سطح ملی و بین‌المللی با کمک تمام نهادها و ارگانهای دولتی بوده است. به همین دلیل وزارت بازرگانی ایران در سال ۱۳۷۴ به عنوان ناظر در چهاردهمین سیات تادل الکترونیک اطلاعات برای امور اداری، تجاری و ترابری (ادیفکت) شروع به فعالیت کرد. در مرداد ۱۳۷۵ با همکاری و مشارکت سازمانهای دیگر مانند گمرک، وزارت راه و ترابری، وزارت پست و تلگراف و بانک مرکزی هیئتی مشابه در ایران تشکیل شد. در حال حاضر تجارت الکترونیک در ایران با استفاده از کارت‌های بانکی چندین بانک عضو شبکه شتاب قابل انجام است. همچنین خدمات بانکداری الکترونیکی نظیر دریافت موجودی و صورت‌حساب، انتقال وجه و پرداخت قبوض آب، برق، گاز، تلفن ثابت و تلفن همراه توسط بانک‌ها در ایران ارائه می‌شود.

قانون تجارت در ایران مشتمل بر هشتاد و یک ماده و هفت تبصره در جلسه علنی روز چهارشنبه مورخ هفدهم دی ماه یکهزار و سیصد و هشتاد و دو مجلس شورای اسلامی تصویب و در تاریخ ۱۳۸۲/۱۰/۲۴ به تأیید شورای نگهبان رسیده است. شش بار مطروحه در قانون تجارت به شرح ذیل می باشد:

- ۱- مقررات عمومی شامل
- ۲- دفاتر خدمات صدور گواهی الکترونیکی
- ۳- در قواعد مختلف
- ۴- جرایم و مجازات ها
- ۵- جبران خسارت
- ۶- متفرقه

عرف بین ال ملی اذعان دارد که قانون تجارت الکترونیکی باید هر سه سال یک بار مورد بازبینی قرار گیرد. تقریباً ۱۱ سال از عمر قانون تجارت الکترونیکی می گذرد اما تاکنون حتی یک بار هم این قانون مورد بازنگری و اصلاح قرار نگرفته است. این قانون جزو اولین قوانینی است که در ایران برای فضای مجازی تدوین شده است همین امر لزوم بازنگری در آن را نشان می دهد. چرا که از آن زمان تاکنون علاوه بر اینکه زیرساخت های ارتباطی تغییر کرده است، بسیاری از فرآیندهای اجرایی و نگاه به فناوری اطلاعات و همچنین ارتباطات دستگاه های اجرایی و دولتی یکدیگر تغییر کرده اند. طبق ماده ۸۰ قانون تجارت الکترونیکی وظیفه بازنگری در این قانون بر عهده مرکز توسعه تجارت الکترونیکی است.

- در اساس نامه مرکز توسعه تجارت الکترونیکی، وظایف زیر به عهده مرکز نهاده شده است:
- ارائه تسهیلات و حمایت از ایجاد و توسعه زیرساخت های فنی، سرمایه های انسانی، قانونی، حاکمیتی و امنیتی توسعه تجارت الکترونیکی.
 - فرهنگ سازی و آموزش فرهنگ تجارت الکترونیکی.
 - توسعه فعالیت های تدارکاتی و معاملاتی به صورت الکترونیکی.
 - حمایت از گسترش بازارهای داد و ستد الکترونیکی.
 - فراهم سازی زمینه تعاملات ملی و بین المللی در تجارت الکترونیکی.

- تسهیل تجارت از طریق ایجاد پنجره واحد.
 - تدوین مقررات، استانداردها و ضوابط مربوط به تجارت الکترونیکی و پیشنهاد به مراجع ذیصلاح برای تصویب.
 - ارایه خدمات صدور گواهی الکترونیکی کشور.
 - ارایه چهارچوب و ضوابط حمایت از مصرف کنندگان در فضای تجارت الکترونیکی.
- باید توجه داشت در بازنگری قانون نباید فقط به تجارت الکترونیکی توجه کرد، باید تمامی بخش‌ها را در نظر گرفت، در اصل باید با یک دید کلی به دولت الکترونیکی نگاه کرد و طبق آن نگاه، به بازنگری قانون اقدام نمود. همچنین در کنار آن باید به زندگی الکترونیکی اشخاص نیز توجه کرد، باید موارد مربوط به حریم خصوصی در فضای الکترونیکی مشخص شود.
- در واقع باید میان راننده داخلی و قوانین بین‌المللی یک هارمونی ایجاد شود و با یک نگاه کل‌نگر اقدام به تدوین بازنگری قانون کرد البته از ملزومات دیگر در وضع قوانین فرهنگ، آداب و سنن یک کشور نیز دخیل می‌باشد که از فاکتورهای مهم در این خصوص است.
- جهت تدوین و تصویب قوانین در حوزه‌های تخصصی بایستی کارگروهی متشکل از خبرگان در تخصص‌های مرتبط با مواد مطروحه به چون مهندسی فناوری اطلاعات، حقوقدان‌ها و ... به گرد یکدیگر درآیند و مواد قانونی و احکام آن را با دید جامع و از منظرهای مختلفی چون اجتماعی، فقهی، سیاسی، فرهنگی و فنی مورد بررسی قرار دهند.
- از این رو در این کتاب مقایسه تطبیقی بین قوانین تجارت الکترونیک ایران و سایر کشورها مورد بررسی قرار گرفته شده است و امید است تا منتهاجی برای پویانگ راه علم فراهم آورد. انشاءالله.

با آرزوی توفیق الهی

محمدصادق محمدی‌فر



۳۷	فصل اول: کلیات
۳۷	۱-۱. اینترنت
۳۸	۲-۱. فناوری اطلاعات
۳۸	۳-۱. سیستم اطلاعات
۴۱	۴-۱. فناوری اطلاعات و قانون
۴۳	۵-۱. تجارت الکترونیک
۴۴	۱-۵-۱. مدل B ₂ B
۴۵	۲-۵-۱. مدل B2C و C2C
۴۵	۳-۵-۱. مدل C2C
۴۵	۴-۵-۱. مدل B2G و G2B
۴۶	۵-۵-۱. مدل G2C و C2G
۴۶	۶-۵-۱. مدل G2G
۴۶	۷-۵-۱. تکنولوژی‌ها و همگرایی با محرک‌های تجاری
۴۷	۸-۵-۱. مشخصات سیستم‌های تجارت الکترونیک
۴۷	۶-۱. قوانین تجارت الکترونیک
۵۱	۷-۱. جرائم رایانه‌ای
۵۱	۱-۷-۱. تاریخچه جرائم رایانه‌ای
۵۴	۲-۷-۱. انواع جرائم سایبری
۵۵	۱-۲-۷-۱. جرائم رایانه‌ای (رایانه موضوع جرم)
۵۶	۲-۲-۷-۱. جرائم مرتبط با رایانه
۵۷	۸-۱. شکاف در قانون جرائم اینترنتی
۵۹	فصل دوم: حاکمیت بر فضای مجازی
۵۹	۱-۲. فضای مجازی
۶۲	۲-۲. حاکمیت قانون و حاکمیت بر فضای مجازی
۶۶	۳-۲. حاکمیت قانون

فصل سوم: تجارت الکترونیک و قانون قراردادهای

- ۱-۳. قوانین و مقررات سایر کشورها
- ۲-۳. قراردادهای الکترونیکی
- ۱-۲-۳. عقود رضایی
- ۲-۲-۳. عقود تشریفاتی
- ۱-۲-۲-۳. منبع تشریفات
- ۲-۲-۲-۳. اشکال تشریفات
- ۳-۲-۲-۳. بررسی امکان تأمین تشریفات در قراردادهای الکترونیکی
- ۳-۲-۳. موافق دو اراده
- ۳-۳-۱. ایجاب
- ۲-۳-۲-۳. دره اعتبار ایجاب
- ۳-۳-۲-۳. فبر
- ۳-۳. اعتبار معاملات الکترونیکی
- ۱-۳-۳. اسناد رسمی الکترونیک و ارزش اثباتی آن
- ۲-۳-۳. سند عادی الکترونیک و ارزش اثباتی آن
- ۱-۲-۳-۳. اسناد الکترونیکی که به صورت مطمئن تهیه و نگهداری شده‌اند
- ۲-۲-۳-۳. اسناد الکترونیکی که به صورت غیر مطمئن تهیه و نگهداری شده‌اند
- ۳-۳-۳. وضعیت حقوقی اسناد الکترونیکی
- ۱-۳-۳-۳. عناصر و ارکان سند الکترونیک
- ۱-۱-۳-۳-۳. قابلیت استناد
- ۲-۱-۳-۳-۳. دستیابی
- ۳-۱-۳-۳-۳. تولید و نگهداری به روش مطمئن
- ۴-۱-۳-۳-۳. امضای الکترونیکی
- ۲-۳-۳-۳. آیا تعامل قابل اعتماد است؟
- ۱-۲-۳-۳-۳. تشخیص اصالت هویت فرستنده
- ۳-۳-۳-۳. تمامیت داده‌ها
- ۴-۳-۳. آثار اسناد الکترونیکی
- ۱-۴-۳-۳. اسناد الکترونیکی در قوانین جهانی و آثار آن
- ۲-۴-۳-۳. آثار اسناد الکترونیکی رسمی

- ۱۰۵ ۳-۳-۴-۱. آثار ثبت اسناد
- ۱۰۶ ۳-۳-۴-۳. آثار اسناد الکترونیکی عادی
- ۱۰۶ ۳-۳-۴-۱. اسناد الکترونیکی که به صورت مطمئن تهیه و نگهداری شده‌اند
- ۱۰۷ ۳-۳-۴-۲. اسناد الکترونیکی که به صورت غیرمطمئن تهیه و نگهداری شده‌اند
- ۱۰۸ ۳-۳-۵. اسناد تجاری الکترونیکی
- ۱۱۳ ۳-۴-۴. نگهداری از اطلاعات و اسناد
- ۱۱۳ ۳-۴-۱. تقسیم‌بندی سازمان‌دهی اسناد
- ۱۱۵ ۳-۵-۵. نگهداری در فرم الکترونیکی
- ۱۱۶ ۳-۵-۱. نحوه عملکرد
- ۱۱۷ ۳-۵-۲. مزایای مشهود
- ۱۱۸ ۳-۶-۶. زمان و محل ارسال و دریافت الکترونیکی
- ۱۱۹ ۳-۶-۱. زمان ارسال
- ۱۱۹ ۳-۶-۲. زمان دریافت
- ۱۱۹ ۳-۶-۳. پذیرش توسط ارتباط الکترونیکی و قوانین پذیرش پستی
- ۱۲۱ ۳-۷-۷. کوچک کردن قراردادها
- ۱۲۱ ۳-۷-۱. Shrink Wrap
- ۱۲۱ ۳-۷-۲. Click Wrap
- ۱۲۲ ۳-۷-۳. Browse Wrap
- ۱۲۲ ۳-۷-۴. عوامل الکترونیکی
- ۱۲۳ ۳-۸-۸. امضای الکترونیکی
- ۱۲۳ ۳-۸-۱. امضای سنتی
- ۱۲۳ ۳-۸-۱-۱. برخی از خواص مهم امضاهای دستی عبارت است از:
- ۱۲۳ ۳-۸-۲. امضای مدرن
- ۱۲۴ ۳-۸-۲-۱. قراردادها و امضاهای الکترونیک
- ۱۲۵ ۳-۸-۲-۲. امضاهای رمزنگاری شده
- ۱۲۵ ۳-۸-۲-۳. امضاهایی بر پایه XML
- ۱۲۵ ۳-۸-۲-۴. انتخاب بین قراردادهای الکترونیک
- ۱۲۶ ۳-۸-۲-۵. قراردادهایی الزاماً کاغذی
- ۱۲۷ ۳-۸-۲-۶. قانون کلی درم قابل قانون جزئی

- ۱۲۷ ۳-۸-۳. امضای الکترونیک
- ۱۲۸ ۱-۳-۸-۳. مشخصات امضای دیجیتال
- ۱۳۰ ۲-۳-۸-۳. امضای دیجیتالی امنیت چه چیزی را تأمین می‌کند؟
- ۱۳۱ ۳-۳-۸-۳. روش ایجاد امضای دیجیتالی
- ۱۳۳ ۴-۳-۸-۳. روش تولید امضای دیجیتالی
- ۱۳۳ ۵-۳-۸-۳. ویژگی‌های امضاهای دیجیتالی
- ۱۳۳ ۶-۳-۸-۳. حملات ممکن علیه امضای دیجیتال
- ۱۳۴ ۷-۳-۸-۳. معایب امضای دیجیتال
- ۱۳۶ ۸-۳-۸-۳. زبانی امضای دیجیتال
- ۱۳۶ ۹-۳-۸-۳. رخی از کاربردهای امضای دیجیتالی
- ۱۳۷ ۴-۸-۳. امنیت امضای الکترونیکی
- ۱۳۸ ۵-۸-۳. اخذ گواهی از CA
- ۱۳۸ ۱-۵-۸-۳. مراکز صدور گواهی نامه (CA: Certificate Authority)
- ۱۳۹ ۲-۵-۸-۳. روال فعالیت مراکز صدور گواهی نامه (CA: Certificate Authority)
- ۱۴۱ ۳-۵-۸-۳. بخش‌های مرکز صدور گواهی نامه
- ۱۴۱ ۴-۵-۸-۳. اهداف CA
- ۱۴۲ ۵-۵-۸-۳. ثبت‌نام برای یک گواهی‌نامه دیجیتالی
- ۱۴۲ ۶-۵-۸-۳. پخش کردن گواهی‌نامه دیجیتالی
- ۱۴۲ ۷-۵-۸-۳. انواع مختلف گواهی‌نامه دیجیتالی
- ۱۴۳ ۸-۵-۸-۳. سطوح مختلف گواهی‌نامه‌های الکترونیکی
- ۱۴۳ ۹-۵-۸-۳. کاربردهای گواهی دیجیتال
- ۱۴۴ ۱۰-۵-۸-۳. قوانین مرتبط در این خصوص
- ۱۴۵ ۱۱-۵-۸-۳. دفاتر ثبت‌نام گواهی الکترونیک: (RA)
- ۱۴۵ ۱-۱۱-۵-۸-۳. از جمله فعالیت‌های دفتر ثبت‌نام
- ۱۴۶ ۱۲-۵-۸-۳. مرکز اعتبار سنجی
- ۱۴۶ ۱-۱۲-۵-۸-۳. خدمات VA (validation authority)
- ۱۴۶ ۲-۱۲-۵-۸-۳. مخزن گواهی‌نامه CA
- ۱۴۶ ۳-۱۲-۵-۸-۳. مخزن CRL
- ۱۴۷ ۴-۱۲-۵-۸-۳. پاسخ OCSP

- ۱۴۷ ۳-۸-۵-۱۳. مدل اعتماد یا ساختار سلسله مراتبی CA چیست
- ۱۴۷ ۳-۸-۵-۱۴. مزیت ساختار سلسله مراتبی چیست
- ۱۴۸ ۳-۸-۵-۱۵. زیرساخت کلید عمومی چیست؟ (PKI)
- ۱۴۸ ۳-۸-۵-۱۵-۱. زیرساخت کلید عمومی PKI
- ۱۴۹ ۳-۸-۵-۱۵-۲. زیرساخت کلید عمومی چه خدماتی را ارائه می‌کند
- ۱۵۰ ۳-۸-۵-۱۵-۳. دایرکتوری کلید عمومی چیست
- ۱۵۱ ۳-۸-۵-۱۵-۴. پارامترهای کلیدی دایرکتوری کلید عمومی
- ۱۵۱ ۳-۸-۵-۱۵-۵. نقاط ضعف و راهکارهای مناسب
- ۱۵۲ ۳-۸-۵-۱۵-۶. پروتکل استعلام برخط وضعیت گواهی
- ۱۵۲ ۳-۸-۵-۱۵-۷. مقایسه OCSP با CRL
- ۱۵۴ ۳-۸-۵-۱۵-۸. Browser، ابزاری که OCSP را پشتیبانی می‌کنند
- ۱۵۴ ۳-۸-۶-۱. لایه سوکتهای امن - امنیت لایه حمل و نقل
- ۱۵۴ ۳-۸-۶-۱. ملزومات یک ارتباط امن - پروتکل امنیتی SSL
- ۱۵۵ ۳-۸-۶-۲. مکانیسمهای تشکیل SSL
- ۱۵۵ ۳-۸-۶-۳. الگوریتمهای رمزنگاری پشتیبانی شده در SSL
- ۱۵۶ ۳-۸-۶-۴. پروتکل Secure Sockets Layer
- ۱۵۷ ۳-۸-۶-۵. پروتکل امنیتی لایه انتقال (Transport Layer Security)
- ۱۵۸ ۳-۸-۶-۶. Secure Electronic Transaction
- ۱۵۸ ۳-۸-۷. کاربردها
- ۱۶۱ **فصل چهارم: مسائل کپی‌رایت در تجارت الکترونیکی**
- ۱۶۱ ۴-۱. ماهیت کپی‌رایت
- ۱۶۳ ۴-۱-۱. قانون کپی‌رایت برای دانشگاهیان ایالات متحده
- ۱۶۴ ۴-۱-۲. تاریخ انقضای کپی‌رایت
- ۱۶۵ ۴-۱-۳. مزایای کپی‌رایت و حقوق مرتبط با آن
- ۱۶۵ ۴-۱-۴. چگونگی همگامی کپی‌رایت با پیشرفت‌های تکنولوژی
- ۱۶۵ ۴-۱-۵. چگونگی تنظیم کپی‌رایت و حقوق مربوط به آن
- ۱۶۶ ۴-۱-۶. کپی‌رایت در اینترنت
- ۱۶۷ ۴-۲. حق تجاری
- ۱۶۸ ۴-۳. حقوق انحصاری

- ۶۹ ۱-۳-۴. حقوق مرتبط با کپی‌رایت
- ۷۰ ۱-۱-۳-۴. حقوق معنوی
- ۷۰ ۲-۱-۳-۴. حقوق مادی
- ۷۰ ۳-۱-۳-۴. حق نشر و تکثیر
- ۷۱ ۲-۳-۴. حقوق مالکیت فکری (حق اختراع یا حق مخترع)
- ۷۲ ۳-۳-۴. حق اختراع چیست؟
- ۷۲ ۱-۳-۳-۴. قیاس حق مؤلف و حق مخترع
- ۷۳ ۴-۴. نقض
- ۷۳ ۱-۴-۴. نشر، پخش و عرضه غیرقانونی
- ۷۳ ۱-۴-۴. استفاده غیرقانونی از نام، عنوان و نشان
- ۷۴ ۵-۴. نرم‌افزار
- ۷۵ ۱-۵-۴. چگونه حمایت قانونی از نرم‌افزارها
- ۷۷ ۲-۵-۴. حقوق مورثان و مایات نامرئی
- ۷۷ ۱-۲-۵-۴. حقوق مادی
- ۷۷ ۱-۱-۲-۵-۴. حق تکثیر
- ۷۸ ۲-۱-۲-۵-۴. حق اجرای اثر
- ۷۸ ۲-۲-۵-۴. ویژگی‌های حقوق مادی
- ۷۸ ۱-۲-۲-۵-۴. موقتی بودن
- ۷۹ ۲-۲-۲-۵-۴. قابل انتقال بودن
- ۱۸۲ ۳-۲-۵-۴. استثنای مهم حقوق مادی: استفاده منصفانه
- ۱۸۴ ۱-۳-۲-۵-۴. قانون حمایت از هنرمندان مصوب ۱۳۴۸
- ۱۸۵ ۴-۲-۵-۴. حقوق معنوی
- ۱۸۵ ۱-۴-۲-۵-۴. حق انتساب
- ۱۸۶ ۲-۴-۲-۵-۴. غیرقابل انتقال بودن
- ۱۸۶ ۳-۴-۲-۵-۴. محدود نبودن به زمان و مکان
- ۱۸۶ ۳-۵-۴. حقوق کیفری و مدنی پدیدآورندگان نرم‌افزارها
- ۱۸۹ ۴-۵-۴. قوانین در انگلیس و فرانسه و ایتالیا

فصل پنجم: علائم تجاری و ثبت اختراعات

- ۱۹۱ ۱-۵. ماهیت علائم
- ۱۹۱ ۱-۱-۵. علامت تجاری
- ۱۹۲ ۲-۱-۵. علائم خدماتی
- ۱۹۲ ۳-۱-۵. علامت جمعی
- ۱۹۳ ۴-۱-۵. علامت تصدیقی
- ۱۹۴ ۲-۵. ثبت علامت
- ۱۹۵ ۱-۲-۵. الزامات ثبت علائم
- ۱۹۶ ۲-۲-۵. علائم قابل ثبت (مجاز)
- ۱۹۶ ۱-۲-۲-۵. علائم بیانی و نوشتنی
- ۱۹۷ ۲-۲-۲-۵. اعداد، حروف و حروف اختصاری
- ۱۹۸ ۳-۲-۲-۵. علائم تصویری
- ۱۹۸ ۴-۲-۲-۵. علائم ویژه و غیرهاده
- ۱۹۹ ۱-۴-۲-۲-۵. علائم صوتی
- ۱۹۹ ۲-۴-۲-۲-۵. علائم بویایی
- ۱۹۹ ۵-۲-۲-۵. علائم خدماتی
- ۱۹۹ ۶-۲-۲-۵. علائم تصدیقی (تأییدکننده یا تضمینی)
- ۲۰۰ ۳-۲-۵. علائم غیرقابل ثبت (ممنوع)
- ۲۰۰ ۱-۳-۲-۵. غیرقابل ثبت به دلیل فقدان ویژگی تمایز بخش
- ۲۰۰ ۱-۱-۳-۲-۵. واژه‌های عمومی یا غیراختصاصی (Generic Terms)
- ۲۰۰ ۲-۱-۳-۲-۵. واژه‌های توصیفی
- ۲۰۱ ۲-۳-۲-۵. غیرقابل ثبت به دلیل منافع عمومی:
- ۲۰۱ ۴-۲-۵. انتقال کامل یا جزئی مالکیت
- ۲۰۱ ۱-۴-۲-۵. فروش
- ۲۰۲ ۲-۴-۲-۵. قرارداد مجوز بهره‌برداری (لیسانس)
- ۲۰۲ ۳-۴-۲-۵. فرانچایز
- ۲۰۳ ۵-۲-۵. مدت حمایت
- ۲۰۳ ۳-۵. اختراع ثبت شده برای نرم افزار و اینترنت پردازش
- ۲۰۴ ۱-۳-۵. مفهوم شرط گام ابتکاری

- ۵-۳-۲. ساختار و رویه‌ی قانون اداره‌ی ثبت اختراعات اروپا
- ۵-۳-۲-۱. ساختار اداره
- ۵-۳-۲-۲. رویه‌ی قانونی
- ۵-۳-۳. ساختار و رویه‌ی قانونی اداره‌ی ثبت اختراع و علائم تجاری آمریکا
- ۵-۳-۳-۱. ساختار اداره
- ۵-۳-۳-۲. رویه‌ی قانونی
- ۵-۳-۴. ساختار و رویه‌ی قانونی اداره‌ی ثبت اختراع ژاپن
- ۵-۳-۴-۱. ساختار اداره
- ۵-۳-۴-۲. رویه‌ی قانونی
- ۵-۳-۵. ساختار و رویه‌ی قانونی اداره‌ی ثبت اختراع ایران
- ۵-۳-۵-۱. ساختار اداره
- ۵-۳-۵-۲. رویه‌ی قانونی
- فصل ششم: اسرار تجاری
- ۶-۱. اسرار تجاری
- ۶-۲. معیارهای تعیین و تشخیص اسرار تجاری
- ۶-۳. جلوگیری از تجاوز و استفاده‌ی بدعهدانه
- ۶-۴. حق انتقال اسرار تجاری به دیگران
- ۶-۵. موافقت‌نامه و قرارداد عدم افشا NDA
- ۶-۶. طول مدت حمایت از اسرار تجاری
- ۶-۷. مقدمات موجود در موافقت‌نامه‌های بین‌المللی
- ۶-۷-۱. GATT
- ۶-۷-۲. World Trade organization
- ۶-۷-۳. Trips
- ۶-۸. مطالعه تطبیقی حمایت از اسرار تجاری در سطح بین‌المللی
- ۶-۸-۱. آمریکا
- ۶-۸-۲. ژاپن
- ۶-۸-۳. برزیل
- ۶-۸-۴. چین
- ۶-۸-۵. هند
- ۶-۹. مقررات داخلی ایران

- ۲۳۶ ۱-۹-۶. مقررات جزایی
- ۲۳۸ ۲-۹-۶. مواد موجود در قانون تجارت الکترونیکی
- ۲۴۱ **فصل هفتم: نام‌های دامنه**
- ۲۴۱ ۱-۷. فضای مجازی نقشه‌برداری
- ۲۴۱ ۱-۱-۷. تعریف نام‌های دامنه
- ۲۴۳ ۲-۱-۷. تفاوت نام‌های دامنه و علائم تجاری
- ۲۴۴ ۳-۱-۷. مسئولیت مدنی در حقوق خارجی
- ۲۴۴ ۱-۳-۱-۷. نظام حقوقی آمریکا
- ۲۴۸ ۱-۱-۳-۱-۷. ضمانت اجرا
- ۲۴۸ ۲-۱-۳-۱-۷. سود و محدودیت‌های اجرای قانون ACPA
- ۲۴۸ ۲-۳-۱-۷. نظام حقوق انگلستان
- ۲۴۹ ۳-۳-۱-۷. شیوه‌نامه مداخله در حل اختلاف سازمان ICANN
- ۲۴۹ ۱-۳-۳-۱-۷. شرایط طرح شکایت و ضمانت اجرا
- ۲۵۰ ۲-۳-۳-۱-۷. تقابل اصل آزادی بیان و حقوق مربوط به نام‌های دامنه
- ۲۵۱ ۴-۳-۱-۷. نظام حقوقی ایران
- ۲۵۲ ۱-۴-۳-۱-۷. علائم تجاری مشمول ماده ۲۲۲ قانون تجارت الکترونیکی
- ۲۵۳ ۲-۴-۳-۱-۷. مبنای حمایت از علائم تجاری در ماده ۲۶
- ۲۵۴ ۳-۴-۳-۱-۷. ضمانت حقوقی نقض علائم تجاری در دستورالعمل‌های الکترونیکی
- ۲۵۵ ۱-۳-۴-۳-۱-۷. استفاده از علامت تجاری به‌عنوان نام دامنه
- ۲۵۶ ۲-۳-۴-۳-۱-۷. نمایش بر خط علائم تجاری
- ۲۵۸ ۲-۷. شناسه‌های کسب‌وکار
- ۲۵۸ ۱-۲-۷. طول دامنه
- ۲۵۹ ۲-۲-۷. به یادآوردن آسان
- ۲۵۹ ۳-۲-۷. پرهیز از اسامی متشابه
- ۲۵۹ ۴-۲-۷. چند باور اشتباه در مورد نام دامنه
- ۲۶۰ ۱-۴-۲-۷. اشباع تمامی نام‌ای دامنه
- ۲۶۰ ۲-۴-۲-۷. جایگزینی پروفایل‌های اجتماعی به‌جای نام‌های دامنه
- ۲۶۰ ۳-۴-۲-۷. رتبه بالاتر COM. نسبت به .NET، .ORG. و غیره در موتورهای جستجو
- ۲۶۱ ۴-۴-۲-۷. قیمت مناسب دامنه دات COM جهت فروش

- ۶۱ ۳-۷. ذات نام‌های دامنه
- ۶۱ ۱-۳-۷. تفاوت پسوندهای دامنه
- ۶۲ ۲-۳-۷. معانی برخی از پسوندهای مختلف دامنه
- ۶۴ ۴-۷. سیاست‌نامه حل اختلاف در زمینه ثبت نام دامنه (ایران)
- ۶۴ ۱-۴-۷. اقرار و قبول مفاد و شرایط سیاست‌نامه
- ۶۵ ۲-۴-۷. لغو ثبت نام دامنه، انتقال و تغییرات نام دامنه
- ۶۵ ۳-۴-۷. الزام به داوری بر اساس سیاست‌نامه حل اختلاف
- ۶۸ ۴-۴-۷. سایر اختلافات و دعاوی
- ۶۹ ۵-۴-۷. خالت، مرکز ثبت در دعاوی
- ۶۹ ۴-۷. پایبندی به حفظ وضع موجود
- ۶۹ ۷-۴-۷. انتقال در سن روز اختلاف
- ۷۰ ۸-۴-۷. تغییرات سیاست‌نامه
- ۷۱ **فصل هشتم: صلاحیت در فضای مجازی**
- ۷۱ ۱-۸. قوانین حقوق بین‌الملل خصوصی
- ۷۳ ۲-۸. صلاحیت برون مرزی در قاذورات مجازی اسلامی
- ۷۴ ۳-۸. صلاحیت درون مرزی مراجع بیفری
- ۷۴ ۴-۸. صلاحیت محلی در قانون آئین دادرسی کیفری
- ۷۶ ۵-۸. چالش‌های قواعد دادرسی سنتی در فضای سایبر
- ۷۶ ۱-۵-۸. نامعین بودن حیطه‌های جغرافیایی
- ۷۷ ۲-۵-۸. صلاحیت قضایی در قبال مجرمین
- ۷۸ ۱-۲-۵-۸. ایالات متحده
- ۸۰ ۲-۲-۵-۸. کشورهای اروپایی
- ۸۰ ۳-۲-۵-۸. کنوانسیون جرائم محیط سایبر - بوداپست ۲۰۰۱
- ۸۲ ۳-۵-۸. مسائل لاینحل
- ۸۳ ۱-۳-۵-۸. تعیین محل ارتکاب جرم سایبر
- ۸۴ ۲-۳-۵-۸. شناسایی تابعیت شخص مرتکب
- ۸۴ ۳-۳-۵-۸. حل تعارض صلاحیت‌ها
- ۸۵ ۴-۳-۵-۸. رویکرد کلی

فصل نهم: نهمت، افترا و توهین در فضای مجازی

- ۲۸۹ ۱-۹. افترا
- ۲۸۹ ۱-۱-۹. عنصر مادی جرم افترا
- ۲۹۰ ۲-۱-۹. عنصر روانی جرم افتراء
- ۲۹۱ ۳-۱-۹. شرایط تحقق جرم افترا
- ۲۹۱ ۱-۳-۱-۹. آنچه شاکی باید ثابت کند به شرح زیر می‌باشد
- ۲۹۲ ۴-۱-۹. چه دفاعیاتی برای مقابله با یک اتهام افترا وجود دارد
- ۲۹۳ ۵-۱-۹. مجازات جرم افتراء در ایران چیست
- ۲۹۳ ۱-۵-۱-۹. افترا به اشخاص حقوقی
- ۲۹۴ ۲-۵-۱-۹. افترا نسبت به اشخاص متعدد
- ۲۹۴ ۳-۵-۱-۹. افتراء مطوعات
- ۲۹۴ ۴-۵-۱-۹. افتراء نسبت به اهرات
- ۲۹۵ ۵-۵-۱-۹. در حکم افتراء بودن تشابه موضوع محاکمه قبل از قطعی شدن حکم
- ۲۹۵ ۶-۵-۱-۹. نسبت دادن زنا یا لواط
- ۲۹۵ ۷-۵-۱-۹. مبدأ مرور زمان در بزه افتراء
- ۲۹۵ ۸-۵-۱-۹. قوانین مرتبط با جرم افتراء
- ۲۹۷ ۲-۹. توهین
- ۲۹۷ ۱-۲-۹. اقسام جرم توهین
- ۲۹۹ فصل دهم: حریم خصوصی و حفاظت از داده‌ها
- ۲۹۹ ۱-۱۰. اطلاعات آزاد
- ۲۹۹ ۲-۱۰. حریم خصوصی
- ۳۰۲ ۱-۲-۱۰. تاریخچه توجه به حق حریم خصوصی
- ۳۰۳ ۲-۲-۱۰. نگاهی به قوانین چند کشور در مورد حریم خصوصی
- ۳۰۳ ۱-۲-۲-۱۰. ایالات متحده آمریکا
- ۳۰۵ ۲-۲-۲-۱۰. جمهوری هند
- ۳۰۶ ۳-۲-۲-۱۰. اردن
- ۳۰۷ ۴-۲-۲-۱۰. جمهوری ترکیه
- ۳۰۸ ۵-۲-۲-۱۰. جمهوری اسلامی ایران
- ۳۰۹ ۶-۲-۲-۱۰. حریم خصوصی در اسلام

- ۱۱ ۱-۲-۳. انواع حریم خصوصی
- ۳۱۱ ۱-۲-۳-۱. حریم خصوصی جسمانی
- ۳۱۱ ۱-۲-۳-۲. حریم خصوصی اطلاعاتی
- ۳۱۲ ۱-۲-۳-۳. حریم ارتباطات
- ۳۱۲ ۱-۲-۳-۴. حریم مکانی
- ۳۱۲ ۱-۲-۴. نقض حریم خصوصی در فضای مجازی
- ۳۱۳ ۱-۲-۵. امنیت شبکه و پیشگیری از نقض حریم خصوصی
- ۳۱۵ ۲-۳. اصول ملی حفظ حریم شخصی کاربران
- ۳۱۶ ۱-۴. حقایق از داده‌ها
- ۳۱۶ ۱-۴-۱. اطلاعات حساس
- ۳۱۶ ۱-۴-۲. دسترسی روز آم / فقط خواندن (Read-Only Access)
- ۳۱۷ ۱-۴-۳. اهمیت و ضرورت امنیت در فضای مجازی
- ۳۱۷ ۱-۴-۴. فناوری‌های امنیت اطلاعات
- ۳۱۸ ۱-۴-۴-۱. طبقه‌بندی FOSSEC
- ۳۲۰ ۱-۴-۴-۲. آسیب‌شناسی و تأمین امنیت در فضای مجازی ایران
- ۳۲۳ ۱-۴-۴-۳. چالش‌ها و موانع اساسی مدیریت امنیت در فضای مجازی و اینترنت
- ۳۲۳ ۱-۴-۴-۴. چالش‌های پیش روی اینترنت در ایران
- ۳۲۵ ۱-۴-۴-۵. راه‌کارها و اقدامات مؤثر بر امنیت فضای مجازی و اینترنت
- ۳۲۷ ۱-۵. کوکی‌ها
- ۳۲۷ ۱-۵-۱. نحوه عملکرد کوکی‌ها
- ۳۲۷ ۱-۵-۲. ایجاد کوکی
- ۳۲۸ ۱-۵-۳. فیلدهای اطلاعاتی کوکی
- ۳۲۸ ۱-۵-۴. انواع کوکی
- ۳۲۹ ۱-۵-۵. موارد استفاده از کوکی
- ۳۳۱ فصل یازدهم: پست الکترونیکی و حضور آنلاین
- ۳۳۱ ۱-۱۱. پست الکترونیک
- ۳۳۱ ۲-۱۱. پروتکل‌ها
- ۳۳۱ ۳-۱۱. تأیید هویت
- ۳۳۲ Confidentiality. ۱-۳-۱۱
- ۳۳۲ Integrity. ۲-۳-۱۱

- ۳۳۲ Availability.۳-۳-۱۱
- ۳۳۴ ۴-۱۱. شرایط لازم جهت انجام مبادلات الکترونیکی ایمن و مطمئن
- ۳۳۵ ۵-۱۱. زبان
- ۳۳۶ ۶-۱۱. ویروس‌ها
- ۳۳۶ ۷-۱۱. تکذیب‌نامه‌ها
- ۳۳۷ ۸-۱۱. خدمات اسناد از طریق ایمیل
- ۳۳۷ ۹-۱۱. گروه‌های خبری و لیست‌های پستی
- ۳۳۷ ۱-۹-۱۱. گروه‌های خبری (usenet)
- ۳۳۹ ۱۰-۱۱. محرمانه
- ۳۳۹ ۱-۱۰-۱۱. اسناد در ایمیل خدمات دهنده بجای ایمیل وب
- ۳۳۹ ۲-۱۰-۱۱. کد کردن ایمیل خود با PGP
- ۳۳۹ ۳-۱۰-۱۱. کد کردن کلاسک
- ۳۴۰ ۴-۱۰-۱۱. کد کردن غیرمستقیم
- ۳۴۱ ۵-۱۰-۱۱. چگونه ایمیل‌مان را محرمانه نگاه داریم
- ۳۴۲ ۱-۵-۱۰-۱۱. مهاجرت به یک سرویس ایمیل امن‌تر
- ۳۴۳ ۲-۵-۱۰-۱۱. استفاده از سرویس RiseUp
- ۳۴۴ ۳-۵-۱۰-۱۱. نکاتی برای بالا بردن سطح امنیت ایمیل
- ۳۴۵ **فصل دوازدهم: جرائم کامپیوتری**
- ۳۴۵ ۱-۱۲. مقدمه
- ۳۴۶ ۲-۱۲. اشتراک قانون، جرم و جنایت کامپیوتری
- ۳۴۸ ۱-۲-۱۲. تعریف شبه جرم
- ۳۴۸ ۲-۲-۱۲. رسیدگی به جرم کامپیوتری
- ۳۴۹ ۳-۲-۱۲. ساختار سازمانی
- ۳۴۹ ۱-۳-۲-۱۲. مسؤولیت بازجویی
- ۳۴۹ ۲-۳-۲-۱۲. تخصیص منابع
- ۳۴۹ ۳-۳-۲-۱۲. گزارش جرائم اینترنتی
- ۳۵۰ ۴-۳-۲-۱۲. صلاحیت قضائی بین‌المللی
- ۳۵۰ ۴-۲-۱۲. اقدامات لازم مبارزه
- ۳۵۰ ۱-۴-۲-۱۲. دسترسی به تکنولوژی
- ۳۵۰ ۲-۴-۲-۱۲. حمایت از علوم قضائی کامپیوتری

- ۳۵۱ ۱۲-۲-۳. آموزش
- ۳۵۱ ۱۲-۲-۵. برنامه‌های نظارت و پیشگیری از وقوع جرائم رایانه‌ای
- ۳۵۲ ۱۲-۲-۵-۱. نقش دادستان برای پیشگیری از وقوع جرائم رایانه‌ای
- ۳۵۳ ۱۲-۲-۵-۲. پلیس فضای تولید و تبادل اطلاعات ایران
- ۳۵۳ ۱۲-۲-۵-۳. نقش مردم در پیشگیری از وقوع جرائم رایانه‌ای
- ۳۵۴ ۱۲-۲-۵-۴. اظهارات جان اشکرافت دادستان ایالت متحده
- ۳۵۶ ۱۲-۲-۶. توصیه‌ها و پیشنهادات
- ۳۵۷ ۱۲-۳-۳. خدمات مخابراتی
- ۳۵۷ ۱۲-۳-۱. خدمات و فضای مجازی
- ۳۵۸ ۱۲-۳-۱۱. تان اینترنتی
- ۳۵۹ ۱۲-۴. پورنوگرافی (زنان)
- ۳۶۲ ۱۲-۵. خودکشی
- ۳۶۳ ۱۲-۵-۱. قوانین مربوط به خودکشی در سایر کشورها
- ۳۶۴ ۱۲-۶. پلیس و قدرت امنیتی
- ۳۶۵ ۱۲-۷. قدرت‌های تحقیقاتی
- ۳۶۵ ۱۲-۸. تخلفات قانونی دولت مربوط به کامپیوتر
- ۳۶۶ ۱۲-۹. اینترنت و قمار
- ۳۶۶ ۱۲-۹-۱. مواد ۷۰۵ تا ۷۱۱ قانون مجازات اسلامی ایران در ارتباط با جرم قمار
- ۳۶۷ ۱۲-۹-۲. مصادیقی از قمار در فضای مجازی
- ۳۶۷ ۱۲-۹-۲-۱. پیش‌بینی مسابقات ورزشی
- ۳۶۸ ۱۲-۹-۲-۲. مسابقات پیامکی
- ۳۶۸ ۱۲-۹-۲-۳. مسابقات قرعه‌ای (بخت‌آزمایی)
- ۳۶۸ ۱۲-۱۰. هرزنامه
- ۳۷۰ ۱۲-۱۰-۱. قانونمند کردن هرزنامه در برخی از کشورها
- ۳۷۲ ۱۲-۱۱. کلاهبرداری
- ۳۷۳ ۱۲-۱۱-۱. ارکان جرم کلاهبرداری کامپیوتری
- ۳۷۳ ۱۲-۱۱-۱-۱. عنصر قانونی
- ۳۷۴ ۱۲-۱۱-۲. عنصر مادی جرم کلاهبرداری کامپیوتری (رایانه‌ای)
- ۳۷۶ ۱۲-۱۱-۱-۱. کلاهبرداری از دیدگاه سایر کشورها
- ۳۷۶ ۱۲-۱۱-۳. عنصر معنوی جرم

- ۳۷۷ ۱۲-۱۱-۱-۴. کیفرهای جرم کلاهبرداری کامپیوتری
- ۳۷۷ ۱۲-۱۱-۱-۴-۱. کیفر کلاهبرداری تام
- ۳۷۹ ۱۲-۱۱-۲. آشنایی با برخی از روش‌های کلاهبرداری اینترنتی در ایران
- ۳۷۹ ۱۲-۱۱-۲-۱. شاهزاده نیجریه‌ای
- ۳۸۰ ۱۲-۱۱-۲-۲. خانه‌های اجاره‌ای
- ۳۸۰ ۱۲-۱۱-۲-۳. دلارهای سیاه
- ۳۸۰ ۱۲-۱۱-۲-۴. کلاهبرداری از زندان
- ۳۸۰ ۱۲-۱۱-۲-۵. چربان دروغ‌گو
- ۳۸۱ ۱۲-۱۱-۲-۶. بده خیالی یا بازنده واقعی
- ۳۸۱ ۱۲-۱۱-۲-۷. کلاهبرداری با داماد آنلاین
- ۳۸۲ ۱۲-۱۱-۲-۸. کلاه‌های بی‌جوشندگان کار
- ۳۸۲ ۱۲-۱۱-۲-۹. فروش کالای تقلبی
- ۳۸۲ ۱۲-۱۱-۲-۱۰. کلاهبرداری به برانده فروش وسایل دست‌دوم
- ۳۸۳ ۱۲-۱۱-۲-۱۱. کلاهبرداری با ایمیل جعلی
- ۳۸۳ ۱۲-۱۱-۲-۱۲. فیس بوک / هات‌میل
- ۳۸۳ ۱۲-۱۱-۲-۱۳. غرامت
- ۳۸۴ ۱۲-۱۱-۲-۱۴. اشتباه
- ۳۸۴ ۱۲-۱۱-۲-۱۵. کلاهبرداری از طریق ترفندهای افزایش سازه
- ۳۸۴ ۱۲-۱۱-۲-۱۶. سایت‌هایی که حراجی اینترنتی نیستند
- ۳۸۵ ۱۲-۱۱-۲-۱۷. روش‌های کلاهبرداری در شبکه‌های اجتماعی
- ۳۸۶ ۱۲-۱۱-۲-۱۸. پول‌شویی الکترونیک
- ۳۸۹ ۱۲-۱۱-۲-۱۹. پول‌شویی بین‌المللی
- ۳۹۱ ۱۲-۱۱-۲-۱۹-۱. قانون مبارزه با پول‌شویی
- ۳۹۴ ۱۲-۱۱-۲-۱۹-۲. آیین‌نامه اجرایی قانون مبارزه با پول‌شویی ایران
- ۴۱۱ ۱۲-۱۱-۲-۲۰. اسکیمینگ
- ۴۱۲ ۱۲-۱۱-۲-۲۰-۱. روش مقابله با اسکیمینگ
- ۴۱۳ ۱۲-۱۱-۲-۲۱. فیشینگ
- ۴۱۴ ۱۲-۱۱-۲-۲۱-۱. روش‌های مختلف و مرسوم فیشینگ
- ۴۱۶ ۱۲-۱۱-۲-۲۱-۲. مقابله با فیشینگ

- ۴۱۷ ۱۲-۱۱-۳. راه‌های پیشگیری از کلاهبرداری
- ۴۲۰ ۱۲-۱۲. تبلیغات
- ۴۲۲ ۱۲-۱۲-۱. تبلیغات تجاری
- ۴۲۳ ۱۲-۱۲-۲. انواع محدودیت‌ها از نظر حقوق مخاطب
- ۴۲۴ ۱۲-۱۲-۳. تاریخچه تبلیغات بازرگانی در جهان
- ۴۲۵ ۱۲-۱۲-۳-۱. در دوران باستان (دوره نخست ارتباطات شفاهی)
- ۴۲۵ ۱۲-۱۲-۳-۲. دوره دوم - دوره ارتباطات نوشتاری - چاپی
- ۴۲۵ ۱۲-۱۲-۳-۳. دوره سوم: دوره ارتباطات الکترونیکی
- ۴۲۶ ۱۲-۱۲-۳-۴. دوره چهارم: دوره ارتباطات دیجیتالی (دوره پایانی قرن ۲۰ به بعد)
- ۴۲۶ ۱۲-۱۲-۴. مسائلی که می‌تواند موجب وضع قانون گردد
- ۴۲۷ ۱۲-۱۲-۵. قوانین ایران و سایر کشورها
- ۴۳۱ ۱۲-۱۳. تقلب در مرز و ترانزیت - رسم - قالب جدید نظارت الکترونیکی ملی
- ۴۳۱ ۱۲-۱۳-۱. تعریف تروریسم - تروریسم مجازی
- ۴۳۱ ۱۲-۱۳-۲. انواع تروریسم
- ۴۳۱ ۱۲-۱۳-۱-۱. تروریسم کلاسیک
- ۴۳۲ ۱۲-۱۳-۲-۲. سایبر تروریسم
- ۴۳۲ ۱۲-۱۳-۲-۱-۱. تاریخچه سایبر تروریسم
- ۴۳۲ ۱۲-۱۳-۲-۲-۲. جذابیت سایبر تروریسم
- ۴۳۴ ۱۲-۱۳-۲-۲-۳. دفاع در برابر سایبر تروریسم
- ۴۳۵ ۱۲-۱۳-۳. قانون ضد تروریسم و مبارزه با تروریسم در ایران و جهان
- ۴۳۵ ۱۲-۱۳-۳-۱. سازمان ملل متحد
- ۴۳۶ ۱۲-۱۳-۳-۲. جرائم تروریستی در حقوق کیفری فرانسه
- ۴۳۸ ۱۲-۱۳-۳-۱-۲. جرائم تروریستی در قانون جزای ۱۹۹۴ فرانسه
- ۴۴۰ ۱۲-۱۳-۳-۳. قانون ضد تروریسم در پاکستان
- ۴۴۲ ۱۲-۱۳-۳-۴. مسائل حقوقی تروریسم در افغانستان
- ۴۴۲ ۱۲-۱۳-۳-۵. قوانین تروریسم در جمهوری اسلامی ایران
- ۴۵۸ ۱۲-۱۳-۴. قانون دستگاه‌های مدار بسته
- ۴۶۰ ۱۲-۱۴. شواهد الکترونیکی (ادله دیجیتالی)
- ۴۶۰ ۱۲-۱۴-۱. مقدمه‌ای بر ادله الکترونیکی

۴۶۰. ۱-۱-۱۴-۱۲. اهمیت ادله الکترونیک
۴۶۱. ۱-۱-۱۴-۱۲. وکلای دادخواهان (شاکیان)
۴۶۳. ۱-۱-۱۴-۱۲. مانوران تعقیب و بازرسان دولت
۴۶۴. ۱-۱-۱۴-۱۲. وکلای خواندگان (متهمان)
۴۶۴. ۱-۱-۱۴-۱۲. علت متفاوت بودن ادله الکترونیک
۴۶۶. ۱-۱۴-۱۲. پست الکترونیک و فرآیند کشف
۴۶۹. ۱۴-۱۲. کشف ادله الکترونیک
۴۷۳. ۱-۲-۱۴-۱۲. مراحل کلی کشف ادله الکترونیک
۴۷۷. ۲-۲-۱۴-۱۲. تفتیش / توقیف سیستم‌های رایانه‌ای
۴۷۷. ۱-۲-۲-۱۴-۱۲. ملاحظات مهم در انجام تفتیش / توقیف
۴۸۲. ۲-۲-۲-۱۴-۱۲. ملاحظات و در پی جویی‌های کیفی
۴۸۴. ۳-۲-۱۴-۱۲. ملاحظات رجوع مع مانگی
۴۸۴. ۴-۲-۱۴-۱۲. نگهداری و مراقبت ز ادله الکترونیک
۴۸۵. ۵-۲-۱۴-۱۲. استخدام متخصص بسایی نامی و تر
۴۸۵. ۱-۵-۲-۱۴-۱۲. کاهش ریسک پیش از شروع دادخواهی / پی جویی
۴۸۶. ۲-۵-۲-۱۴-۱۲. بعد از شروع دادخواهی / تفتیش
۴۸۹. ۶-۲-۱۴-۱۲. انتخاب متخصص جنایی رایانه
۴۹۰. ۷-۲-۱۴-۱۲. هزینه خدمات بازیابی داده‌های رایانه‌ای
۴۹۱. ۳-۱۴-۱۲. آیین‌نامه جمع‌آوری و استناد پذیری ادله الکترونیک در ایران
۵۰۰. ۱۵-۱۲. راه‌هایی برای جلوگیری از جرائم هدفمند بر فضای مجازی
۵۰۰. ۱-۱۵-۱۲. جرائم اینترنتی، پیشگیری و مقابله
۵۰۳. ۲-۱۵-۱۲. مفهوم پیشگیری وضعی
۵۰۵. ۱-۲-۱۵-۱۲. تدابیر محدودکننده یا سلب‌کننده دسترس
۵۰۶. ۲-۲-۱۵-۱۲. نظارت شبکه‌ای
۵۰۶. ۳-۲-۱۵-۱۲. تدابیر صدور مجوز
۵۰۷. ۴-۲-۱۵-۱۲. ابزارهای ناشناس کننده و رمزگذاری
۵۰۸. ۳-۱۵-۱۲. داده‌کاوی و کشف جرم و سیستم‌های اطلاعات جغرافیایی
۵۰۸. ۱۶-۱۲. پیشنهاداتی اصلاحی در حوزه‌ی قانون جرائم رایانه‌ای ایران
۵۰۸. ۱-۱۶-۱۲. تهمت و افترا در فضای مجازی و شبکه‌های اجتماعی

- ۰۹ ۱۲-۱۶-۲. قذف
- ۰۹ ۱۲-۱۶-۳. تدلیس در تجارت الکترونیکی
- ۰۹ ۱۲-۱۶-۴. مغفول ماندن چند مصداق
- ۰۹ ۱۲-۱۶-۵. آموزش شیوه‌های هک
- ۱۰ ۱۲-۱۶-۶. وضعیت تبلیغات کذب
- ۱۰ ۱۲-۱۶-۷. عدم وجود برخی از مصادیق
- ۱۰ ۱۲-۱۶-۸. جریمه با نوع جرم تناسب ندارد
- ۱۰ ۱۲-۱۶-۹. مجوزهای فروش
- ۱۰ ۱۲-۱۶-۱۰. سمبل‌های خاص
- ۱۱ ۱۲-۱۶-۱۱. اطلاعات سایت جز حریم خصوصی است یا خیر؟
- ۱۱ ۱۲-۱۶-۱۲. عدم همپوشانی برخی قوانین
- ۱۱ ۱۲-۱۶-۱۳. درگاه پرداخت واسطه
- ۱۲ ۱۲-۱۶-۱۴. شیوه‌های برداشت غیررسمی
- ۱۲ ۱۲-۱۶-۱۵. برگه ایمیل - اثرات اعتباری جهت ارائه قانون
- ۱۲ ۱۲-۱۶-۱۶. وضعیت تعاملات جبرانی
- ۱۲ ۱۲-۱۶-۱۷. مالکیت معنوی نام اینترنتی
- ۱۳ ۱۲-۱۶-۱۸. عدم آگاهی خریدار به حقوق قانونی خود و ارائه‌دهنده
- ۱۳ ۱۲-۱۶-۱۹. صفحات تبلیغاتی و کلیک دزدی
- ۱۳ ۱۲-۱۶-۲۰. مزاحمت‌های اینترنتی
- ۱۳ ۱۲-۱۶-۲۱. تعیین تکلیف وضعیت حقوقی وبلاگ‌ها
- ۱۳ ۱۲-۱۶-۲۲. هفت روز ضمانت بازگشت وجه
- ۱۴ ۱۲-۱۶-۲۳. لاگ گیری فعالیت‌های اینترنتی
- ۱۵ ۱۲-۱۶-۲۴. پول‌شویی - کار شویی
- ۱۷ **فصل سیزدهم: حاکمیت سانسور و پخش محتوی آنلاین**
- ۱۷ ۱۳-۱. تعریف و تاریخچه‌ای از سانسور
- ۲۲ ۱۳-۲. تعریف خودسانسوری
- ۲۳ ۱۳-۳. انواع سانسور
- ۲۵ ۱۳-۴. تاریخچه‌ای از قوانین سانسور اینترنت در سایر کشورها
- ۲۵ ۱۳-۴-۱. آمریکا

۵۲۹	۱۳-۴-۲. فرانسه
۵۳۰	۱۳-۴-۳. انگلیس
۵۳۲	۱۳-۴-۴. ایتالیا
۵۳۲	۱۳-۴-۵. آلمان
۵۳۳	۱۳-۴-۶. استرالیا
۵۳۵	۱۳-۴-۷. کانادا
۵۳۶	۱۳-۴-۸. چین
۵۳۷	۱۳-۴-۹. عربستان سعودی
۵۳۸	۱۳-۴-۱۰. ژاپن
۵۳۹	۱۳-۴-۱۱. سرریه
۵۳۹	۱۳-۴-۱۲. اردن
۵۳۹	۱۳-۴-۱۳. مراکش
۵۴۰	۱۳-۴-۱۴. امارات
۵۴۰	۱۳-۴-۱۵. بحرین
۵۴۰	۱۳-۴-۱۶. هندوستان
۵۴۵	منابع و مراجع