موسسه آموزش عالی فروردین قائم شهر

Farvardin Institute of Higher Education

جزوه درس:

حقوق فضای مجازی

گردآورنده:

جناب آقای فرشاد دارایی

موسسه آموزش عالی فروردین قائم شهر

نکات کلیدی شماره (۱)

- فضای مجازی نخستین بار توسط ویلیام گیبسون و در سال ۱۹۸۴ به کار گرفته شد.
- فضای مجازی عامل محوری تحقق دهکده جهانی است.
- رایانه یا کامپیوتر افزاری است که برای انجام عملیات‌های محاسباتی یا منطقی به کار می‌رود.
- آنچه امروزه منجر به قابل تصور شدن فضای مجازی شده ست، دو پدیده رایانه و اینترنت می‌باشد.
- هر رایانه متشکل از مجموعه‌ای از سخت‌افزارها، نرم‌افزارها و سفت‌افزارها می‌باشد.

نکات کلیدی شماره (۲)

- رایانه‌های اولیه سه ویژگی داشتند: ۱. فضای زیادی را اشغال می‌کردند، ۲. کند بودند، ۳. تنوع و دامنه عملیات آن‌ها به شدت محدود بود.
- رایانه‌های مدرن از سه ویژگی برخوردارند: ۱. از مدارهای یکپارچه برخوردار بودند، ۲. از رایانه‌های قدیمی تندتر هستند، ۳. فضای کمی را اشغال می‌کنند.
- در مقایسه با برنامه رایانه‌ای، نرم‌افزارها مفهوم عام‌تری دارند و منظور از نرم‌افزار بخش‌هایی از رایانه می‌باشد که شکل مادی ندارند.

نکات کلیدی شماره (۳)

- زمانی که نرم‌افزار در حافظه سخت (هارد) ذخیره نشود به نحوی که تغییر در آن به سختی ممکن باشد، به آن سفت‌افزار می‌گویند.
- بدافزار به معنای هر برنامه یا شیوه حمله مجازی است که بر علیه برنامه‌های معمول رایانه‌ای یا شبکه‌های کامپیوتری به کار گرفته می‌شود.
- انواع عمده بدافزارها عبارتند از: ویروس، کرم رایانه‌ای، نامه ناخواسته، اسب تروا، بمب منطقی، بوکش‌ها، حمله قطع خدمات و تارتن‌ها.

نکات کلیدی شماره (۴)

- بدافزارها در جزئیات فنی یا شیوه تهاجم با یکدیگر متفاوتند.
- ویروس، معروف‌ترین بدافزاری است که در زمینه رایانه وجود دارد.
- کرم‌های رایانه‌ای از ویروس‌ها خطرناک‌ترند.
- وسیله جابجایی کرم‌ها، اغلب نامه الکترونیکی است.
- هکرها به منظور مقاصد مجرمانه و تکثیر و پخش ویروس از نامه‌های ناخواسته استفاده می‌کنند.
- از نامه‌های ناخواسته برای اهداف ضدفرهنگی مانند روابط نامشروع، شرطبندی، تبلیغ قمار و ... استفاده می‌شود.

نکات کلیدی شماره (۵)

- هکرها اغلب از اسب‌های تروا به منظور انتقال ویروس استفاده می‌کنند.
- بوکش‌ها ابزاری برای دسترسی به رمزهای ورود، اطلاعات شخصی و شماره کارت‌های اعتباری به شمار می‌آیند.
- برخی از تارتن‌ها توانایی ربودن داده از تارنماهای مجاز را دارند.
- در سال ۱۹۸۳، پروتکل اینترنتی به عنوان تنها شیوه مجاز برای انتقال داده در شبکه به تصویب رسید.
- پروتکل اینترنتی امکان مبادله برابر اطلاعات را از سوی تمام رایانه‌ها فراهم نمود.

نکات کلیدی شماره (۶)

- نقطه شروع استفاده از اینترنت، سال ۱۹۹۱ بود؛ یعنی زمانی که شبکه بنیاد ملی علوم تصمیم گرفت که موانع تجاری موجود بر سر راه استفاده از اینترنت را بردارد.
- حقوق فضای مجازی به عنوان گرایش مستقل وجود ندارد.
- حقوق فضای مجازی گرایش بین رشته‌ای محسوب می‌شود.
- حقوق فضای مجازی تنها درسی در رشته حقوق است که مباحث حقوقی مرتبط با فضای مجازی در آن مطرح می‌شود.

نکات کلیدی شماره (۷)

- حقوق فضای مجازی با گرایش‌های مختلف از جمله حقوق خصوصی، حقوق مالکیت فکری، حقوق کیفری، حقوق بین‌الملل و حقوق عمومی ارتباط دارد.
- حقوق فضای مجازی اصالت لازم برای تبدیل شدن به یک گرایش ولو فرعی از حقوق را ندارد.

یادداشت

نکات کلیدی شماره (۱)

- قراردادهایی که با موضوع نرم‌افزار یا طراحی، راهبردی و اداره سامانه‌های رایانه‌ای منعقد می‌شود، مشمول قواعد عمومی قرارداد می‌باشد.
- سخت‌افزار نوعی کالا محسوب می‌شود.
- ماهیت قرارداد ارادی و آزادانه است و قرارداد همواره می‌تواند به عنوان یک عامل راهگشا یا محدودکننده در رابطه طرفین به کار گرفته شود.
- به موجب قسمتی از ماده ۹ آیین‌نامه اجرایی مواد ۲ و ۱۷ قانون نرم‌افزار، حقوق مادی و معنوی نرم‌افزار به پدیدآورنده تعلق دارد.

نکات کلیدی شماره (۲)

- اگر در بسته‌بندی نرم‌افزار شروط قراردادی درج شده باشد، مصرف‌کننده با خرید نرم‌افزار به مفاد آن شروط ملتزم می‌شود و نمی‌تواند مدعی جهل به آن‌ها شود.
- حقوق مادی و معنوی نرم‌افزار به پدیدآورنده تعلق دارد.
- حقوق مادی نرم‌افزاری که با سفارش پدید می‌آید به مدت ۳۰ سال به سفارش دهنده تعلق می‌گیرد مگر اینکه به مدت کمتر یا ترتیب محدودتری توافق شده باشد.
- حقوق معنوی نرم‌افزاری که با سفارش پدید می‌آید، متعلق به پدیدآورنده است.

نکات کلیدی شماره (۳)

- بهره‌گیری نادرست یا مغرضانه از رایانه می‌تواند مسئولیت‌زا باشد.
- قرارداد سفارش نرم‌افزار را نمی‌توان پیش‌خرید دانست.
- مفاد قرارداد سفارش نرم‌افزار با توافق طرفین تعیین می‌شود.
- پدید آمدن نرم‌افزار ممکن است ناشی از استخدام یا قرارداد باشد.
- احتمال انعقاد قرارداد اجاره برنامه رایانه‌ای، در مورد آن دسته از برنامه‌های رایانه‌ای است که نیاز طرف قرارداد به آن‌ها موقت بوده و بهای خرید آن بسیار زیاد است.
- قرارداد اعطای مجوز به کاربر نهایی میان شرکت سازنده نرم‌افزار و کاربر منعقد می‌گردد و شروع به استفاده (نصب) نرم‌افزار از سوی کاربر به معنای قبول آن است.

نکات کلیدی شماره (۴)

- نرم‌افزار مجموعه‌ای از اطلاعات است که نسبت به آن مالکیت فکری وجود دارد.
- حقوق مالکیت فکری در مفهوم عام، به ندرت در معاملات مربوط به کالا مطرح می‌شود.
- حقوق مالکیت فکری در قراردادهایی که موضوع آن برنامه‌ها و اطلاعات رایانه‌ای است، می‌تواند مطرح شود.
- برخلاف کتاب یا نوار ویدئویی که خواندن یا تماشا کردن آن از سوی اشخاصی غیر از خریدار، نمی‌تواند نقض حقوق مالکیت فکری به حساب آید، نرم‌افزار دارای این ویژگی است که نصب بدون مجوز آن از سوی کاربر واحد هم می‌تواند نقض حق مالکیت فکری پدیدآورنده آن باشد.

نکات کلیدی شماره (۵)

- قرارداد، بهترین ابزار برای پیشگیری از نقض حق نسبت به نرم‌افزار، حق اختراع، اسرار تجاری و مالکیت فکری و صنعتی محسوب می‌شود.
- بهترین نوع حمایت از اسرار تجاری در روابط استخدامی، انعقاد توافقنامه صریح با موضوع «تعهد به رازداری» است.
- قراردادهای محدودکننده برای پیشگیری از نقض حقوق اسرار تجاری عبارتند از: قرارداد عدم رقابت، قرارداد عدم ترغیب و قرارداد رازداری.

نکات کلیدی شماره (۶)

- به موجب قرارداد عدم رقابت، مستخدم متعهد می‌شود که پس از خاتمه رابطه استخدامی، با استفاده از اسراری که در زمان استخدام به آنها دسترسی پیدا کرده، اقدام به رقابت با کارفرمای سابق خود ننماید.
- به موجب قرارداد عدم ترغیب، طرفین در برابر یکدیگر متعهد می‌شوند تا برای مدت متعارف و در محدوده خاصی، مشتریان و مستخدمین همدیگر را برای تعاملات تجاری با خود یا دیگری ترغیب و تحریک نکنند.
- قرارداد عدم ترغیب، میان رقبای بالفعل یا بالقوه منعقد می‌شود.

نکات کلیدی شماره (۷)

- به موجب قرارداد عدم افشاء، یکی از طرفین متعهد می‌شود که اطلاعات مربوط به طرف دیگر را محرمانه نگه دارد و از آن‌ها به سود خود یا دیگری استفاده نکند.
- اگر در رابطه میان مالک اسرار تجاری و دارنده اسرار تجاری قراردادی به منظور حفظ اسرار تجاری وجود نداشته باشد، می‌توان از قواعد مسؤولیت قهری برای حمایت از اسرار بهره گرفت.
- بسیاری از حوادث را به طور مستقیم یا غیرمستقیم به نقص سامانه‌های هوشمند می‌توان نسبت داد.
- بهترین نوع حمایت از اسرار تجاری در روابط استخدامی، انعقاد توافقنامه صریح با موضوع «تعهد به رازداری» است.

نکات کلیدی شماره (۸)

- قراردادهای محدودکننده برای پیشگیری از نقض حقوق اسرار تجاری عبارتند از: قرارداد عدم رقابت، قرارداد عدم ترغیب و قرارداد رازداری.
- خسارت به سخت‌افزار می‌تواند مسئولیت مدنی عامل را در پی داشته باشد.
- نقض حقوق اسرار تجاری به یکی از سه شکل دستیابی، افشا و به‌کارگیری قابل تصور است.
- دارا شدن ناعادلانه اسرار تجاری در مفهوم عرفی و حقوقی آن زمانی محقق می‌شود که موجد نفع مادی یا معنوی برای دارنده آن باشد.
- «تصاحب ناحق» شرط تحقق «دارا شدن ناعادلانه» محسوب می‌شود.

نکات کلیدی شماره (۱)

- امضاء در لغت در سه معنا به کار می‌رود: ۱. علامتی که پای نامه یا برنامه می‌گذارند، ۲. نوشتن نام خود در زیر نامه یا سند به منزل اقرار یا تصدیق، ۳. صحه گذاشتن و تصدیق امضای یک سند به عنوان متعهد، بر: ۱. انتساب، ۲. انجام تشریفات، ۳. تصدیق، ۴. قدرت اجرایی دلالت دارد.
- منظور از انتساب آن است که با امضای سند، مفاد آن به امضاکننده منتسب می‌شود و او نمی‌تواند مدعی شود که از تمام یا بعضی از محتوایی که امضا نموده بی‌اطلاع است.

نکات کلیدی شماره (۲)

- امضای سند دلالت بر این امر دارد که تمام تشریفات لازم برای تهیه آن سند طی شده است.
- منظور از تصدیق آن است که در نظر عرف، امضای یک سند به معنای تأیید محتوای آن از سوی شخصی است که آن را به عنوان متعهد امضا کرده است.
- منظور از قدرت اجرایی آن است که سندی که امضا می‌شود، به عنوان عقد، ایقاع، اقرار و ... علیه امضاکننده دلیل محسوب می‌شود.
- امضاء در صورتی قانونی است که دلالت بر تأیید تمامی مفاد سند نماید.

نکات کلیدی شماره (۳)

- امضای الکترونیکی عبارت است از هر نوع علامت منضم شده یا به نحو منطقی متصل شده به «داده پیام» است که برای شناسایی امضاءکننده، مورد استفاده قرار می‌گیرد.
- اصل کارکرد یکسان که در رابطه میان نوشته کاغذی و نوشته الکترونیکی، در ماده ۶ ق.ت.ا کشورمان و ماده ۷ قانون نمونه ۱۹۹۶ پذیرفته شده، در مقایسه میان امضای سنتی و امضای الکترونیکی هم اجرا می‌شود.
- یوتا، امکان امضای دیجیتالی وصیت‌نامه و قراردادهای امانی را غیرممکن اعلام نموده است.

نکات کلیدی شماره (۴)

- یوتا، با طرح بحث «قصد امضا» به عنوان شرط امضای الکترونیکی، گامی بلند در مقایسه با دستورالعمل تجارت الکترونیکی و دستورالعمل امضاهای الکترونیکی اروپا و دو قانون نمونه (۲۰۰۱ و ۱۹۹۶) آنسیترال برداشته است.
- در فرانسه، دفاتر ثبت ازدواج نمی‌توانند از امضای الکترونیکی استفاده نمایند.
- تفاوت سند رسمی و عادی در آن است که نسبت به سند رسمی یا سندی که دارای اعتبار سند رسمی است، ادعای انکار یا تردید مسموع نیست همچنین تاریخ تنظیم سند رسمی، برخلاف سند عادی نسبت به اشخاص ثالث هم اعتبار دارد.

نکات کلیدی شماره (۵)

- از نظر اثباتی تنها امضای دیجیتالی می‌تواند واجد شرایط امضای الکترونیکی مطمئن باشد.
- امضای دیجیتالی، محصول علم رمزنگاری است.
- مؤسسه ملی استاندارد آمریکا، استاندارد خاصی را برای رمزنگاری و رمزگشایی داده تصویب کرده و آن را «الگوریتم رمزگذاری داده» نامیده است.
- برای ایجاد متن و امضای مطمئن از تابع هش استفاده می‌شود.
- فایده رمزگذاری دیجیتالی آن است که حتی اگر امضاءکننده کنترل کلید خصوصی را از دست بدهد (آن را فراموش کند)، باز هم امکان جعل آنچه قبل‌تر ایجاد شده وجود نخواهد داشت.

نکات کلیدی شماره (۶)

- حضور فیزیکی نزد سردفتر این امکان را برای سردفتر مهیا می‌سازد که سلامت روانی شخص را احراز نماید و سردفتر مطمئن شود که شخص متقاضی تحت تأثیر اکراه یا اجبار نیست.
- علی‌الاصول نمی‌توان هویت شخص را به شیوه الکترونیکی احراز کرد.
- منظور از «الکترونیکی کردن فرایند کاغذی» آن است که در خصوص اسنادی هم که به شکل کاغذی تهیه می‌شوند می‌توان قسمتی از فرایند تنظیم سند یا اقدامات پس از تنظیم را به شیوه الکترونیکی انجام داد.

نکات کلیدی شماره (۷)

- مزایای اثر انگشت الکترونیکی عبارت است از: ۱. ارزان بودن تهیه و ذخیره، ۲. کم حجم بودن، ۳. کاربرد زیاد آن در روابط تجاری، ۴. قابلیت تهیه نسخه کاغذی از آن.
- «دلیل الکترونیکی» در مفهوم عام به هر نوع اطلاعاتی که در قالب دیجیتالی ایجاد یا ذخیره شده باشد، می گویند.
- ادله الکترونیکی، از آن جهت که: ۱. در جایی ذخیره می‌شوند، ۲. قابل چاپ هستند، ۳. اغلب به صورت مستند می‌توان آن‌ها را ارائه داد، به سند شباهت دارند.

نکات کلیدی شماره (۸)

- ادله رایانه‌ای را می‌توان به ادله در صحنه و ادله پشت صحنه تقسیم‌بندی نمود.
- با استناد به ماده ۱۲۵۸ قانون مدنی، ادله اثبات دعوا در امور مدنی محصور در اقرار، شهادت، سند، اماره و قسم می‌باشد.
- قواعد ادله ایالات متحده نسخه چاپی از محتوای تارنما را در صورتی دارای اصالت می‌داند که صحت، روز و ارتباط آن به وسیله یک شاهد گواهی شود.

نکات کلیدی شماره (۹)

- دادگاه‌های آمریکا، از پذیرش فایل‌های مربوط به اتاق گفتگو (چت‌روم) که مورد ویرایش قرار گرفته خودداری نموده و آن‌ها را فقط در صورتی قابل پذیرش دانسته‌اند که در همان قالب اولیه ارائه شوند.
- اگر «سوابق و گزارش‌های عمومی الکترونیکی» توسط سازمان صادرکننده یا مقام مجاز آن مهر یا امضاء یا تصدیق شده باشد، اصالت آن محرز است.

نکات کلیدی شماره (۱۰)

- اگر «اطلاعات و سوابق شغلی و تجاری» به طور کامل به وسیله رایانه ایجاد شده باشد، مشروط به اینکه سالم بودن دستگاه محل تردید نباشد، اصالت داده‌ها محرز خواهد بود.
- منظور از «ادله الکترونیکی غیرمتنی» آن دسته از ادله الکترونیکی می‌باشد که در قالب «نوشته» نباشد.
- ادله الکترونیکی غیرمتنی را می‌توان به دو دسته مطمئن و غیرمطمئن تقسیم‌بندی نمود.
- امضای الکترونیکی می‌تواند وسیله‌ای برای ارتقای امنیت سند باشد، اما لزوماً شرط اعتبار یا «مطمئن بودن» آن نیست.

نکات کلیدی شماره (۱۱)

- داده‌هایی را که عرفاً قابل مقایسه با نوشته «متن» نیستند را می‌توان از حیث سندیت، «در حکم نوشته» محسوب نمود.
- هرگاه مطمئن بودن دلیل الکترونیکی توسط استنادکننده اثبات نشود می‌توان اصالت آن و امکان استناد به آن به عنوان دلیل را پذیرفت.
- ارزیابی و تعیین ارزش اثباتی ادله الکترونیکی توسط کارشناس مربوطه انجام می‌گیرد.
- دادرس، به عنوان صادرکننده رأی قاطع در هر دعوا، مهمترین و آخرین شخصی است که در خصوص ارزش و تأثیر ادله الکترونیکی حق اظهارنظر دارد.

یادداشت

.....
.....
.....
.....
.....
.....
.....
.....
.....

* نحوه استفاده از نکات کلیدی:

نکات کلیدی شماره (۱)

- قانون جرایم رایانه‌ای، به جرم‌انگاری اعمال مجرمانه‌ای می‌پردازد که در ارتکاب آن‌ها از رایانه استفاده می‌شود یا موضوع آنها سامانه‌های رایانه‌ای، مخابراتی یا داده باشد.
- جرایم فضای مجازی را می‌توان به سه دسته تقسیم‌بندی نمود:
۱. جرایم سنتی: که ممکن است در ارتکاب آن‌ها از رایانه یا دیگر سامانه‌های ارتباطی و مخابراتی استفاده شود مانند کلاهبرداری.
۲. جرایم مرتبط با محتوا: که از جمله شامل نقص حقوق مالکیت فکری نسبت به داده محتوا و هرزه‌نگاری می‌شود.
۳. جرایم علیه تمامیت رایانه و سامانه‌های ارتباطی.

نکات کلیدی شماره (۲)

- قانون جرایم رایانه‌ای در سال ۱۳۸۸ تصویب شد.
- در قانون جرایم رایانه‌ای، تعریفی از جرایم رایانه‌ای نشده است.
- از نظر وزارت دادگستری ایالات متحده، جرم رایانه‌ای هر جرمی را شامل می‌شود که برای ارتکاب، تحقیق و بازرسی یا دادرسی نسبت به آن از فناوری رایانه استفاده شود.
- در مفهوم عام، داده‌های رایانه‌ای شامل اطلاعات مجرمانه و برنامه‌ها و مدارک موجود در رایانه می‌باشد.
- داده‌های رایانه‌ای از نظر قانون و عرف ارزش مالی دارد.
- داده‌های رایانه‌ای اصولاً تحت مالکیت دارنده رایانه می‌باشند.

نکات کلیدی شماره (۳)

- دارنده رایانه، بر داده‌های رایانه‌ای استیلای مشروع دارد و حق انتفاع از آنها و یا انتقال آن‌ها را دارد.
- قانون جرایم رایانه‌ای فقط به جرایم رایانه‌ای اختصاص ندارد بلکه جرایمی که از طریق سامانه‌های مخابراتی یا بر علیه این سامانه‌ها ارتکاب می‌یابد را هم در بر می‌گیرد.
- در فقه استفاده نمودن از حیوان، شخص محجور و یا هر وسیله‌ای برای ارتکاب جرم سرقت بررسی شده و صراحتاً بیان شده که چنین اعمالی، مانع از صدق عنوان سرقت نسبت به عامل جرم نمی‌شود.

نکات کلیدی شماره (۴)

- منظور از سرقت مرتبط با رایانه، ربایش بدون مجوز داده‌های متعلق به غیر می‌باشد.
- «قصد محروم کردن دایمی» به کامن‌لا اختصاص ندارد و در باب مسئولیت مدنی، از جمله مشترکات حقوق حمایت از داده و اطلاعات در تمام دنیا محسوب می‌شود.
- باید مواردی را که علی‌رغم استیلای مالک بر مال، به دلیل فعل غیرمجاز دیگری، آن مال ارزش اقتصادی خود را به طور کامل از دست داده است را «در حکم از بین رفتن و سرقت مال» محسوب نمود.

نکات کلیدی شماره (۵)

- یکی از جرایمی که فضای مجازی می‌تواند پوشش خوبی برای آن محسوب شود و حتی آن را به صورت سازمان یافته در آورد، پول‌شویی است.
- «قانون مبارزه با پولشویی» در سال ۱۳۸۶ به تصویب مجلس شورای اسلامی رسیده است.
- روش‌هایی که از آن برای پول‌شویی استفاده می‌شود عبارتند از:
۱. سرمایه‌گذاری در تجارت الکترونیکی
۲. انتقال الکترونیکی یا اینترنتی وجوه به دست آمده از معاملات نامشروع به حساب‌های متمرکز متعلق به بزهکار یا سایر اشخاص.

نکات کلیدی شماره (۶)

- واژه «ترور» نخستین بار به موجب ماده اول کنوانسیون پیشگیری و مجازات تروریسم وارد ادبیات سازمان‌های بین‌المللی شد.
- تعریف اموال تروریستی عبارت است از: وجوه نقدی که
۱. قرار است برای مقاصد تروریستی مورد استفاده قرار گیرد.
۲. از منابع مالی سازمانی غیرقانونی ناشی شده باشد.
۳. از فعالیت‌های تروریستی حاصل شده باشد.
- هدف تأمین مالی تروریسم دستیابی به اطلاعات مالی و امنیتی و وارد ساختن صدمه اساسی به نظم و منافع عمومی از طریق ابزارهای نوین اطلاعاتی و ارتباطی است.

نکات کلیدی شماره (۷)

- «سامانه رایانه‌ای» عبارت است از هر دستگاه یا مجموعه‌ای از دستگاه‌های متصل یا مرتبط با هم که تمام یا برخی از آنها، طبق یک برنامه، پردازش خودکار داده را انجام می‌دهد.
- دسترسی غیرمجاز به سامانه‌های الکترونیکی، به طور قطع محرمانگی اطلاعات موجود در آن‌ها را در معرض خطر قرار می‌دهد.
- هدف از جرم‌انگاری دسترسی غیرمجاز، مبارزه با اقداماتی همچون هک یا کرک کردن است.

نکات کلیدی شماره (۸)

- رمزگیری، در صورتی که تنها با هدف جرایم مالی انجام گیرد، جرم خاصی به شمار می‌آید که معادل دقیقی در قوانین موضوعه کشورمان برای آن وجود ندارد.
- استفاده از هویت دیگران در پرداخت‌های اینترنتی، اغلب در قالب رمزگیری انجام می‌گیرد.
- سرقت هویت معمولاً به منظور ارتکاب جرایمی مانند کلاهبرداری و تقلب انجام می‌گیرد و به دلیل تعدد مادی ارکان این جرایم در مقایسه با سرقت هویت، مجازات هر دو جرم در مورد شخص اعمال می‌شود.

* نحوه استفاده از نکات کلیدی:
۱- [illegible]

نکات کلیدی شماره (۹)

- رکن مادی جرم دسترسی غیرمجاز، دسترسی بدون مجوز به داده‌ها یا سامانه‌های رایانه‌ای می‌باشد.
- برای سرقت هویت در حقوق موضوعه کشورمان، نمی‌توان معادل خاصی یافت.
- رکن قانونی جرم کلاهبرداری در حقوق جزای کشورمان، ماده ۱ قانون تشدید مجازات مرتکبین ارتشاء و اختلاس و کلاهبرداری است.
- هر گاه جرم اخلال یا تخریب داده، با هدف به خطر انداختن امنیت و آسایش عمومی ارتکاب یابد، مجازات مرتکب حبس از سه سال تا ده سال خواهد بود.

نکات کلیدی شماره (۱۰)

- هرزه‌نگاری در اینترنت و به طور کلی، استفاده از رایانه و ارتباطات رایانه‌ای برای روابط نامشروع، مبادله عکس و فیلم با صدای مبتذل، امروزه یکی از چالش‌های مشترک علوم انسانی (از جمله جامعه‌شناسی، روانشناسی و اخلاق و حقوق) محسوب می‌گردد.
- با استناد به اصل قانونی بودن جرم و مجازات، دریافت محتویات مستهجن از اینترنت یا دریافت از طریق بلوتوث یا پیامک چند رسانه‌ای را نمی‌توان جرم و مشمول مجازات دانست (به دلیل سکوت قانون در خصوص مصادیق ذکر شده).

نکات کلیدی شماره (۱۱)

- فحشا و بهره‌کشی از انسان، مدرن‌ترین شکل برده‌داری است. در این شیوه زنان، دختران و حتی پسرانی از تمام نقاط دنیا، به منظور بهره‌کشی جنسی (غیرارادی) یا روسپیگری (ارادی)، قاچاق می‌شوند.
- نقطه شروع «تروریسم جنسی»، وسایل نوین ارتباطی است.
- نقش سازمان‌های مردم نهاد (NGO) را در پیشگیری از قربانی شدن کودکان و حمایت بعدی از آنها نباید انکار کرد.
- نقض یا تعرض یا نادیده گرفتن حقوق کودکان در فضای مجازی، صرفاً محدود به بهره‌کشی و سوء استفاده نیست.

یادداشت

.....
.....
.....
.....
.....
.....
.....
.....
.....

* نحوه استفاده از نکات کلیدی: