Article

Elements of Cybercrimes in the Penal Code of Afghanistan: An Exploration

Kardan Journal of Law
1 (1) 25–47

Kardan Publications
Kabul, Afghanistan
DOI: 10.31841/KJL.2021.2
https://kardan.edu.af/Research/kardan_journal_of_law.aspx

Ahmad Fardeen Bakhtyari

Abstract

Cybercrimes, unlike other crimes, are crimes that take place in the cyber space. States strive to ensure a safe cyberspace for the users and Afghanistan is no exception. The newly adopted Penal Code is the most comprehensive legislation regulating crimes in Afghanistan and for the first time in history of this country, it covers cybersecurity and cybercrimes. It is vital because the rise of internet as a component of technological advancement has created new opportunities as well as challenges that undermine the safety and security of the cyberspace. This paper analyzes eight acts that are criminalized by the Penal Code of Afghanistan and the elements of these crimes in sufficient detail. It finds out that the legislature has, in many cases, tried to define each crime and lay down its elements. In cases where definition is not included in the Code, focus is shifted to the major elements of crimes. In addition, it is observed that although the Code has laid emphasis on the legal and material elements in certain crimes, such as cyber terrorism and cyber espionage, the mens rea *can only be inferred from the context of each crime.*

Keywords: *Cybercrimes, Penal Code, Data, Elements, Punishment*

Mr. Ahmad Fardeen Bakhtyari *is Lecturer at the Faculty of Law, Kardan University.*

واکاوی عناصر تکوینی
جرایم سایبری در پرتو کود جزای افغانستان

احمد فردین بختیاری

چکیده

جرایم سایبری عبارت از جرایم است که در محیط سایبر بوقوع می پیوندد. ظهور و پیشرفت خیره کننده و روز افزون انترنت به عنوان یکی از مؤلفه های پیشرفت فناوری فرصت ها و چالش های جدیدی را فراروی علوم گوناگون در سپهر های متفاوت فردی و اجتماعی به وجود آورده است. با در نظرداشت خصایص انحصاری فضا و جرایم سایبری از قبیل گسترده بودن، سهولت در ارتکاب، وسعت ضرر، بلند بودن رقم سیاه، مشکلات در کشف، تعقیب و تحقق، ضرور است از فضای سایبر و کاربران در فضای سایبر محافظت صورت گیرد تا مصؤنیت فضا و کاربران سایبر محفوظ بماند. در این مقاله نویسنده به دنبال این است تا جرایم را که در کود جزای افغانستان جرم انگاری شده است، بیان نموده عناصر تکوینی در جرایم مورد نظر را تحت بررسی قرار دهد. یافته های این تحقیق بیان می دارد که قانونگذار افغانستان نهایت تلاش نموده تا هر یک از جرایم را تعریف و عناصر تشکیل دهنده آن را جداگانه بازتاب دهد، حتی در مواردی که اگر به تعریف جرم نپرداخته است ولی تلاش نموده تا مصادیق آن را بیان دارد. با آن که تاکید روی عناصر قانونی و مادی جرایم شده، ولی از فحوای کلی هر ماده می توان جایگاه عنصر معنوی را نیز دریافت، بگونه مثال در تروریزم و جاسوسی سایبری .

واژگان کلیدی: *جرایم سایبری، کود جزا، اطلاعات، عناصر تشکیل دهنده جرم، مؤیدات جزائی*

احمد فردین بختیاری، استاد پوهنځی حقوق، پوهنتون کاردان

مقدمه

پیشرفت تکنولوژی، علم و دست یابی بشر به فناوری اطلاعات، استفاده از کمپیوتر و پیدایش دنیای مجازی دارای پیامدهای مثبت و منفی برای بشر بوده است.[۱] از جمله پیامدهای منفی آن، پیدایش جرایم سایبری می باشد. در مورد جرایم سایبری تعاریف متعددی ذکر شده است، که از جمله پولیس جنایی فدرال آلمان در تعریفی از جرایم سایبری بیان داشته است «جرم سایبری در برگیرنده همه اوضاع، احوال و کیفیاتی است که در آن شکل های پردازش الکترونیك اطلاعات، وسیله ارتکاب و یا هدف یك جرم قرار گرفته است و مبنای برای نشان دادن این ظن است که جرمی ارتکاب یافته است».[۲] همچنان، شورای اروپا در سال ۱۹۸۹ در گزارش کاری یکی از متخصصان جرایم سایبری را چنین تعریف نموده که «هر فعل مثبت غیر قانونی که کمپیوتر، ابزار یا موضوع جرم باشد. به عبارت دیگر هر جرمی که ابزار یا هدف آن تاثیر گذاری برعملکرد کمپیوتر باشد».[۳]

با آنکه تاریخ دقیق از اولین جرم سایبری محض در افغانستان واضح نیست، ولی بحث جرایم سایبری در افغانستان ابتداً درسال ۲۰۱۲مطرح گردیده است. اولین جرم سایبری محض، رخنه گری یا دسترسی غیر مجاز (هکینگ)[٤] به وبسایت شورای امنیت ملی کشور در اوایل ماه مارچ سال ۲۰۱۲ از سوی رخنه گران یا هکرهای منسوب به گروه القاعده می باشد. هکرها این وبسایت را در کنترول خود گرفتند و عکس اسامه بن لادن را در صفحه اول آن قرار دادند. وبسایت شورای امنیت ملی افغانستان بار دیگر به تاریخ ۲۵ نوامبر سال ۲۰۱٦ به وسیله گروه‌ای سایبری که خود را موسوم به ارتش سایبری هزارستان یاد می کنند، مورد حمله دسترسی غیر مجاز قرار گرفته، و برای مدتی تصاویر حنیف اتمر مشاور پیشین امنیت ملی افغانستان، معصوم استانکزی رئیس پیشین امنیت ملی، گل نبی احمدزی فرمانده پیشین

---

[۱] مهدی فضلی، *مسؤولیت کیفری در فضای سایبر* (تهران: انتشارات خرسندی، ۱۳۸۹)، ٦٤.

[۲] حسن عالی پور، *حقوق کیفری فناوری اطلاعات* (تهران: انتشارات خرسندی، ۱۳۹۴)، ۱۰۴.

[۳] محمد رضا زندی، *تحقیقات مقدماتی در جرایم سایبری* (تهران: انتشارات جنگل، ۱۳۹۱)، ٥٦.

[٤] در این مقاله واژه های رخنه گری، دسترسی غیر مجاز یا هک کردن تحت عین مفهوم بکار رفته است و رخنه گر با هکر در ترادف به تذکر گرفته شده است.

گارنیزیون کابل و عبدالرحمن رحیمی فرمانده پیشین پولیس کابل را توأم با بیرق داعش در صفحه شورای امینت قرار داده، سیستم و ارتباطات شبکه انترنیتی سرور شورای امنیت ملی را غیر فعال ساخته بودند. حمله سایبری دسترسی غیر مجاز بالای حساب کاربری تویتر داکتر عبدالله عبدالله، رئیس اجرائیه افغانستان، به تاریخ ۳۱ جولای ۲۰۱۶ نمونه دیگر از حملات سایبری در افغانستان بحساب می رود.

به تاریخ ۲۳ اگست ۲۰۱۳، یک کارمند بانک خصوصی در تبانی با یکی از شرکای جرمی اش در خارج مبلغ یک میلیون و یک صد هزار دالر امریکایی را به حساب یکی از نزدیکان‌اش بگونه غیر قانونی انتقال داد، که لوی څارنوالی افغانستان نیز این رویداد را تأیید نمود. برعلاوه، در سال گذشته وبسایت‌های وزارت خارجه، بانک مرکزی، ارگان‌های محل، وبسایت ولایت بلخ و چندین وبسایت دولتی دیگر و همچنان وبسایت موسسه اکبر و بانک های خصوصی هک شده و در محتوای این وبسایت‌ها تغییراتی آورده شده‌اند.

مقاله حاضر واکاوی و تحلیل عناصر تکوینی هفت جرم از مجموع جرایم جرم انگاری شده در کود جزای افغانستان می نماید، علت گزینش این جرایم، وقوع آنها در بستر افغانستان، قربانی گیری بیشتر آن ها، بالا بودن رقم سیاه این جرایم، عدم اطلاعات کافی کاربران سایبری از وسایل و تدابیر امنیتی برای محافظت از اطلاعات در حریم خصوصی و اجتماعی در برابر این گونه جرایم، و کم هزینه بودن ارتکاب این گونه جرایم می باشد. بنا بر این عوامل، این مقاله به بیان و تشریح کلیه جرایم سایبری موجود در کود جزا نه پرداخته، به واکاوی بعضی از جرایم سایبری بسنده نموده است.

۲- دسترسی غیر مجاز به سیستم، برنامه یا اطلاعات کمپیوتری

جرم دسترسی غیر مجاز بعنوان یکی از جرایم سایبری محض بحساب رفته، در حقیقت این جرم مادر جرایم سایبری[۵] عنوان می گردد. چون از یک لحاظ خود بعنوان یکی از جرایم مستقل و محض سایبری است، و از طرف دیگر مقدمه‌ی برای بیشترین جرایم سایبری می تواند عنوان شود. هرگاه شخصی که به صورت غیر مجاز به اطلاعات، برنامه یا سیستم

[۵] عالی پور، *حقوق کیفری فناوری اطلاعات* ، ۱۵۹.

کمپیوتری محفوظ شده‌ی شخص دیگری بگونه غیر قانونی دسترسی پیدا نماید، جرم دسترسی غیر مجاز متحقق می گردد.

۲-۱ عنصر قانونی جرم

ماده‌ی ۸۵۲ کود جزای افغانستان[۶] بیان می دارد، شخصی که به صورت غیر مجاز به سیستم، برنامه یا اطلاعات کمپیوتری متعلق به دیگری، دسترسی حاصل کند، به حبس قصیر[۷] محکوم به مجازات می گردد. فقره دوم این ماده صراحت دارد، شخصی که به اثر ارتکاب جرم دسترسی غیر مجاز به سیستم، برنامه یا اطلاعات کمپیوتری ضرر جسمی، مالی یا معنوی به شخص یا اشخاص وارد کند، علاوه به حبس قصیر به جزای جرم مرتکبه نیز محکوم می گردد. این را می توان به عنوان عنصر قانونی جرم مذبور بحساب آورد.

۲-۲ عنصر مادی جرم

اصل در تحقق عنصر مادی جرم دسترسی غیر مجاز در کود جزا بر محور تحقق اجرائیوی یا مثبته مطرح می باشد، نه بگونه اهمالی یا منفی آن. موضوع این جرم همانا اطلاعات، برنامه یا سیستم های کمپیوتری می باشد. البته کود جزای افغانستان شرط را مطرح کرده است که باید این گونه دسترسی غیر قانونی بوده باشد، اما شرط محفوظ بودن (Secured) اطلاعات، برنامه یا سیستم های کمپیوتری که در کلیه اسناد بین المللی بشمول کنوانسیون جرایم سایبری (بودابست)[۸] و قوانین کشور ها مطرح گردیده است، را لحاظ ننموده است.

---

[۶] کود جزا ۱۳۹۶، جریده رسمی (۱۲۶۰).

[۷] بر اساس ماده ۱۴۷ کود جزای افغانستان حبس به پنج نوع تقسیم گردیده است: حبس قصیر (از سه ماه تا یک سال)؛ حبس متوسط (بیش از یک سال تا پنج سال)؛ حبس طویل (بیش از پنج سال تا شانزده سال)؛ حبس دوام درجه ۲ (بیش از شانزده سال تا بیست سال) و حبس دوام درجه ۱ (بیش از بیست سال تا سی سال).

[۸] کنوانسیون جرایم سایبر، مصوب جلسه وزاری شورای اروپا هشتم نوامبر ۲۰۰۱ در کنفرانس بین المللی جرایم سایبر در شهر بوداپست می باشد. این کنوانسیون که از چهار فصل و ۴۸ ماده تشکیل گردیده است نخستین کنوانسیون در سطح جهان است که به جرایم سایبری می پردازد. ماده دوم این کنوانسیون صراحت دارد که:

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent,

۲-۳ عنصر روانی جرم

بر اساس ماده‌ی ۸۵۲ کود جزا دو مورد را از لازمه های عنصر روانی در تحقق جرم دسترسی غیر مجاز می توان به حساب آورد. نخست، درک و اگاهی مرتکب از این که چنین دسترسی یک دسترسی غیر مجاز و غیر قانونی می باشد، و دوم، این گونه دسترسی غیر مجاز به اطلاعات، برنامه یا سیستم شخص یا اشخاص دیگر صورت گرفته باشد.

۲-۴ مؤیدات جزائی جرم

در ذیل ماده‌ی ۸۵۲ کود جزا افغانستان، دو رویکرد مؤیده‌ای در خصوص مرتکبین جرم دسترسی غیر مجاز در نظر گرفته شده است. در صورت تحقق مصداق های فقره‌ی (۱) این ماده، مرتکب به حبس قصیر محکوم به مجازات می گردد. و در صورت که از اثر ارتکاب عمل جرمی فقره‌ی (۱)، ایجاد ضرر جسمانی، مالی یا معنوی به شخص یا اشخاص وارد گردد، حالات مشدده قابل اعمال است، که بر علاوه تطبیق جزای حبس قصیر جزای جرم مرتکبه نیز بالای مرتکب اعمال خواهد گردید.

۳- تغییرات غیر مجاز در سیستم، برنامه یا اطلاعات کمپیوتر

موارد نه گانه که درین جا به بحث گرفته می شود، مصادیق ماده های ۸۵۲، ۸۵۳ و ۸۵۴ کود جزا افغانستان را شامل می گردد.

۳-۱ غیرمجاز بودن و عمومی نبودن

بر اساس هدایت فقره ماده‌ی ۸۵۲ و ماده های ۸۵۳ و ۸۵۴ کود جزای افغانستان، دسترسی شامل ورود به تمام یا بخشی از سیستم کمپیوتری، یعنی سخت افزار، اجزای آن، اطلاعات ذخیره شده، در سیستم نصب شده، شاخه ها، اطلاعات ترافیک و اطلاعات مرتبط با محتوا، می شود. دسترسی شامل ورود به سیستم کمپیوتری دیگری بوسیله شبکه های مخابراتی

---

or in relation to a computer system that is connected to another computer system.

ترجمه: هر یک از اعضا باید به شکل اقدام به وضع قوانین و سایر تدابیر نماید، که در صورت لزوم بر محور حقوق داخلی، دسترسی عمدی بدون حق را به کل یا بخشی از یک سیستم، کمپیوتری جرم انگاری نماید، اعضا می توانند مقرر دارند این جرم با نقض تدابیر امنیتی و به قصد تحصیل اطلاعات کمپیوتری یا سایر مقاصد ناروا یا نسبت به سیستم کمپیوتری که با سیستم کمپیوتری دیگری ارتباط دارد، محقق شود.

عمومی یا ورود به سیستم کمپیوتری همان شبکه می شود، نظیر شبکه محلی یا انترنت داخلی یک سازمان نحوه بر قراری ارتباط اهمیتی ندارد. بگونه مثال از راه دور، شامل خطوط بی سیم یا در طیف بسته.

همچنان این عمل باید بدون حق انجام شود ورنه دسترسی مجاز شمرده می شود که از سوی مالک یا ذی حق دیگر به سیستم یا بخشی از آن جرم محسوب نمی شود، مانند دسترسی با هدف ارزیابی مجاز یا حفاظت از سیستم کمپیوتری مورد نظر. علاوه بر این، دسترسی به سیستم کمپیوتری که برای عموم آزاد و رایگان است نیز جرم نیست، ولذا این ذی حق تلقی می شود.[۹]

بکار گیری ابزار های فنی خاص می تواند منجر به دسترسی موضوع ماده‌ی ۸۵۲ تا ۸۵۴ گردد. مانند دسترسی مستقیم یا بوسیله پیوند های فرا متن به صفحه‌ی وب که شامل پیوند های عمیق می شود، یا استفاده از کوکی ها یا بات ها جهت مکان یابی و بازیابی اطلاعات به جای ارتباطات بکارگیری چنین ابزار های به خودی خود بدون حق نیستند. داشتن یک وب سایت عمومی رضایت ضمنی دارنده را مبنی بر دسترسی هر کاربر وب نشان می دهد. بکارگیری ابزار های استاندارد تهیه شده بر پایه پروتکل ها و برنامه های ارتباطات مشترک به خودی خود بدون حق نیست، به ویژه در جایی که فرض می شود صاحب حق سیستم دسترسی یافته این گونه بهربرداری را پذیرفته و برای مثال نصب مقدماتی کوکی ها را رد و آنها را پاک نکرده است.

۳-۱-۱ تغییر وارد کردن

بر محور بند ۱ ماده ۸۵۳ کود جزای افغانستان یکی دیگراز رفتار های تحقق جرم دسترسی غیر مجاز تغییر وارد نمودن به اطلاعات حفاظت شده می باشد. به این مفهوم، هرگاه شخصی به کمپیوتر دیگری دسترسی غیر مجاز پیدا نماید، و بدون اجازه وی و بدون این که کمپیوتر مذکور در استفاده همگان قرار داشته باشد، به اطلاعات شخصی دسترسی پیدا می کند، و در اطلاعات آن تغییر شکلی یا ماهوی بوجود می آورد، این گونه تغییر آوردن یکی از

[۹] امیر حسین جلالی فراهانی، *کنوانسیون جرایم سایبری و پروتکل الحاقی آن* (تهران: انتشارات خرسندی، ۱۳۸۹)، ۲۶.

مصادیق تحقق رفتار مجرمانه جرم دسترسی غیر مجاز بحساب می رود.[۱۰] لازم به تذکر است که تغییر به معنی دستکاری اطلاعات موجود نیز آمده است. بنابر این، وارد کردن کود های مغرضانه، مانند ویروس ها و اسپ های تروا، مشمول این ماده‌ی کود جزای افغانستان می گردد، چون تغییر اطلاعات را منجر می شود.

از طرف دیگر، هرگونه اطلاعات و برنامه های که در حال انتقال باشد، و رخنه گر (هکر) بدون اجازه و رضایت ذی حق به آن دسترسی پیدا نموده و اطلاعات در حال انتقال را تغییر دهد، این گونه تغییر خود از جمله مصادیق تحقق عنصر مادی جرم دسترسی غیر مجاز به حساب می رود.

۳-۱-۲ مختل کردن اطلاعات

بر محور بند ۱ ماده ۸۵۳ و بند ۱ ماده ۸۵۴ کود جزای افغانستان، آسیب رساندن و تخریب به عنوان اعمال هم پوشانیده ای هستند که بطور خاص تغییر منفی تمامیت یا محتوای اطلاعات و برنامه ها دارند. حذف اطلاعات معادل از بین بردن یک شی مادی است.

متوقف کردن اطلاعات کمپیوتری به معنی هر فعلی است که از دسترس پذیری اطلاعات برای شخصی که به کمپیوتری یا حامل اطلاعات که اطلاعات بر روی آن ذخیره شده و به آن ها دسترسی دارد، جلوگیری می کند یا پایان می بخشد.[۱۱] باید خاطر نشان ساخت، موارد فوق زمانی جرم حساب می شوند و قابل مجازات می باشند، که بدون حق و توأم با عمد ارتکاب یافته باشند.

۳-۱-۳ مختل کردن سیستم

بر محور بند ۲ ماده ۸۵۳ و بند ۱ ماده ۸۵۴ کود جزای افغانستان، و توصیه نامه شماره ۸۹ کنوانسیون جرایم سایبری (بوداپست)،[۱۲] از این جرم به خراب کاری کمپیوتری تعبیر شده است. هدف از وضع، جرم انگاری مختل کردن عمدی استفاده قانونی از سیستم های

---

[۱۰] فراهانی، *کنوانسیون جرایم سایبری* ، ۲٦.

[۱۱] مختار فتاحی، بررسی عناصرتشکیل دهنده مادی و معنوی مصادیق جرایم رایانه ای، *فصلنامه علمی-حقوقی قانون یار* (۲: ٦ (۱۳۹۷)، ۱۰٦.

[۱۲] کنوانسیون جرایم سایبری (بودابست)، توصیه نامه ۹ (۸۹) ، ۲۰۰۱.

کمپیوتری است که شامل تجهیزات مخابراتی بوسیله اطلاعات کمپیوتری یا تاثیرگذار بر آنها می شود. منافع قانونی مورد حمایت، مشمول متصدیان و کاربران سیستم های کمپیوتری یا مخابراتی می شود تا بتوانند بطور شایسته فعالیت کنند، این متن به شکل خنثی تنظیم شده تا تمامی انواع کارکرد ها راتحت حمایت قرار دهد.

بر اساس ماده ۸۵۳ کود جزای افغانستان، مختل کردن می تواند به اعمال اطلاق شود که در کارکرد مناسب سیستم کمپیوتری مداخله کرده باشد. این کار با وارد کردن، انتقال دادن ، آسیب رساندن، حذف کردن، تغییر دادن یا متوقف کردن اطلاعات کمپیوتری انجام می شود. بر علاوه، لازم است که مختل کردن شدید باشد تا باعث رویکرد جزائی شود. بطور مثال، کود های زیان بار، نظیر ویروس های که از عملیات سیستم جلوگیری کرده یا سرعت آن را به نحو چشمگیری کاهش می دهند، یا برنامه های که مقادیر زیادی کمپیوتر را برای گیرنده می فرستد، تا کارکرد های ارتباطی سیستم را متوقف کنند.

شرط دیگر اینست که مختل کردن باید بدون حق باشد. فعالیت های معمول ذاتی طراحی شبکه ها یا اقدامات تجاری یا اجرایی معمول به حق است، مانند آزمایش امنیت سیستم کمپیوتر یا حفاظت از آن توسط مالک یا متصدی مجاز شمرده شده یا پیکربندی دوباره سیستم عامل به هنگامی که متصدی سیستم نرم افزار جدیدی را نصب می کند، و برنامه های مشابه نصب شده پیشین را از کار می اندازد. از این رو این اعمال طبق این ماده جرم نیستند، حتی اگر موجب اختلال شدید شوند.

۳-۱-۴ سؤ استفاده از دستگاه ها

بر محور بند ۳ ماده ۸۵۳ و بند ۱ ماده ۸۵۴ کود جزای افغانستان، ارتکاب این جرایم بیشتر مستلزم تصاحب ابزار های دسترسی هکر ها یا سایر ابزار هاست. گرایش زیادی برای بدست آوردن این ابزار ها جهت تحقیق اهداف مجرمانه وجود دارد، و ممکن است به ایجاد نوعی بازار سیاه در تولید و توزیع آنها منجر شود. رخنه گران به وسیله دستگاه های که بعد از هک کردن در دسترسی می داشته باشند، می توانند به هر منظور که خواسته باشند، از دستگاه ها استفاده سؤ بنمایند. مثلاً، میتواند آن را در دسترس ساختن طیاره ها حین پرواز عنوان کرد، یا رخنه کردن در راکت های دور برد عنوان کرد، که رخنه گران بعد ازتسلط حاصل نمودن بالای

این دستگاه ها بهینه ترین استفاده را می توانند انجام بدهند. جهت مبارزه موثرتر با چنین خطر های حقوق جزا باید اعمال و رویکرد های را پیش بین گردد، تا مبارزه مؤثر را بمیان آورده، و این خطرها را از بنیه خنثی نماید.

۳-۱-۵ بوسیله دریافت پاسورد یا شفر

چنان که در ماده ۸۵۲ کود جزای افغانستان تسجیل می گردد، هرگاه شخصی به صورت غیر مجاز به سیستم ، برنامه یا اطلاعات کمپیوتری دیگری دسترسی پیدا نماید، این دسترسی ممکن بوسیله دریافت پاسورد یا رمز شخص محقق گردد. پاسورد شفر همان کلمه، کلمات، اعداد یا همه آنها می توانند باشند که زمینه دسترسی غیر مجاز به سایرین را محدود می گرداند، و در واقعیت امر یکی از اسلوب ها برای حمایت و بلند بردن امنیت اطلاعات، برنامه و سیستم های کمپیوتری می تواند، باشد.

امروزه دانشمندان فناوری اطلاعات اصرار به مغلق بودن، چند رقمی یا ترکیبی بودن پاسوردها یا شفرها (پاسورد های مغلق) می نمایند، چون هر قدر پاسورد مغلق و چند رقمی و ترکیبی باشد، رخنه کردن به آن توسط رخنه گران را به مشکل مواجه می سازد. بنابرین باید نهایت تلاش صورت گیرد، که در حین گزینش پاسورد یا شفر، از پاسورد های کار گرفته شود که مغلق باشند، و با مؤلفه ها ومناسبت های شخصی صاحب پاسورد، از قبیل تخلص خانوادگی، تاریخ تولد، یا نشانی خانه و یا موارد دیگر که به نحوی به صاحب پاسورد همخواهی دارد، نباشد.

۳-۱-٦ ذریعه پخش و انتشار ویروس

در فقره ٦ ماده ۸۵۳ کود جزای افغانستان عبارت «وارد نمودن یا پخش ویروس در سیستم، برنامه یا اطلاعات کمپیوتری» به ذکر گرفته شده است. از نص این ماده چنین استنباط می گردد، که یکی از جلوه های تبلور عنصر مادی جرم دسترسی غیر مجاز وارد نمودن، پخش و انتشار ویروس می باشد.

هکرها، که شامل افراد با درایت و فهم بالایی در بخش فناوری اطلاعات و دانش کمپیوتری می باشند، دست به تولید ویروس زده، و به اشکال گوناگون ویروس ها را آماده می سازند، و بوسیله انترنت که شبکه های متعدد را در سطح جهان به هم پیوست نموده است، انتشار

داده، و ملیون ها و ملیارد ها کاربر را آسیب پذیر می سازند. بگونه مثال یک ویروس به نام I Love You ساخته و بوسیله انترنت به شبکه های جهانی انتقال و پخش گردید، که در نتیجه بیشتر از ۱۱ میلیارد دالر به افراد بشر زیان مالی بوجود آورد.[۱۳] فلهذا یکی از شیوه های تحقق عنصر مادی جرم دسترسی غیر مجاز انتقال و پخش ویروس بوسیله انترنت می باشد.

۳-۱-۷ بسته رمز دار

یکی از راه های دیگر تحقق عنصر مادی جرم دسترسی غیر مجاز بسته رمز دار می باشد. بسته رمز دار به این مفهوم که هکرهای که حوصله زیاد دارند، بگونه تصادفی و اتفاقی چند بار با نام های مختلف و رمز های متخلف خواهان رخنه به حساب کاربر می گردد، و ممکن با این شیوه نیز سیستم، برنامه یا اطلاعات شخص دیگر مورد دسترسی غیر مجاز قرار گیرد. فلهذا جلوه دیگر از تحقق عنصر مادی جرم دسترسی غیر مجاز بسته رمزدار است.

۳-۱-۸ رقص موش

شیوه‌ی دیگر از تحقق عنصر مادی جرم رقص موش می باشد. رقص موش به این مفهوم است که یک رخنه گر بگونه سرگرمی یا اتفاقی بعضی کودها و نام ها را وارد می نمایند و ممکن یکی از این کود ها یا شفر به حساب کاربری صدق نماید، و به این شکل وی به اطلاعات یا برنامه یا سیستم شخص دسترسی پیدا نماید. این ها سبب تحقق عنصر مادی جرم دسترسی غیر مجاز می گردد. کاربرد کلمات همچو دسترسی، تغییر وارد کردن، ممانعت کردن، آسیب رساندن، غیر قابل دسترس ساختن، بی معنا کردن، غیر قابل استفاده ساختن، جلوگیری از دسترسی مجاز، وارد نمودن یا پخش ویروس یا دسترسی غیر مجاز در مسیر اتصال شبکه، همه دال بر تحقق عنصر مادی جرم دسترسی غیر مجاز بحساب می رود.

۳-۲ عنصر قانونی جرم

مادام که قانون گذار فعل یا ترک فعلی را جرم نشناسد و مجازات برای آن تعیین نکند افعال انسان مباح است. بنابر این، تحقق جرم و صدور حکم مجازات منوط به نص صریح قانون

[13] Neal K. Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003 (2001). Available online at: <https://scholarship.law.upenn.edu/penn_law_review/vol149/iss4/2> (Last Accessed: 20.12.2019).

است. وچون بدون وجود قانون جرم محقق نمی شود، گزاف نیست که گفته شود قانون رکن لازم جرم است.[۱۴] از طرف دیگر عنصر قانونی به تعریف چیستی یک جرم در حدود قانون می پردازد، نه صرفاً به بیان مصداق های یک جرم. ولی بگونه‌ی تلویحی می توان ماده‌ی ۸۵۳ کود جزای افغانستان را به مثابه عنصر قانونی تغییرات غیر مجاز در سیستم، برنامه یا اطلاعات کمپیوتری به حساب آورد.

۳-۳ عنصر مادی جرم

از جمله موضوعات و مصداق های که بعنوان عنصر مادی در جرم متذکره بحساب می رود، کود جزای افغانستان به هفت مورد آن چه طور مؤقت باشد یا دائمی به قرار ذیل در ماده ۸۵۳ اشاره نموده است:

۱. تغییر وارد نمودن، تعدیل یا آسیب رساندن به سیستم، برنامه یا اطلاعات کمپیوتری
۲. تولید، تغییر، تعدیل یا آسیب رساندن به سیستم، برنامه یا اطلاعات کمپیوتری
۳. غیر قابل دسترسی ساختن، بی معنا کردن، غیر قابل استفاده ساختن، یا غیر فعال نمودن سیستم، برنامه یا اطلاعات کمپیوتری
۴. جلوگیری از دسترسی مجاز به سیستم، برنامه یا اطلاعات کمپیوتری
۵. آوردن تغییر یا تعدیل در سیستم محافظتی، برنامه یا اطلاعات کمپیوتری
٦. وارد نمودن یا پخش ویروس در سیستم برنامه یا اطلاعات کمپیوتری
۷. دسترسی غیر مجاز در مسیر اتصال شبکه کمپیوتری

در خصوص توضیح فقرهفتم ماده‌ی ۸۵۳ کود جزا که می توان تحت عنوان شنود غیرمجاز نیز یاد آور شد، همچون دسترسی غیرمجاز ناشی از عدم رضایت دارنده واقعی یا قانونی اطلاعات یا محتوای در حال انتقال می باشد. همچنین شرط غیرقانونی بودن نیز به شرط رضایت اضافه می شود. این جرم در واقع تعرض به حریم ارتباطات به وسیله شنود سنتی و ضبط مکالمات تلیفون افراد را بیان می کند. باید تذکر داده شد که موضوع جرم در شنود

[۱۴] محمد علی اردبیلی، *حقوق جزای عمومی* (تهران: نشر میزان، ۱۳۹۲)،۱۲٦.

غیرمجاز محتواست.[۱۵] برای محتوا ویژگی در حال انتقال پیش بینی شده است، یعنی این جرم تنها اطلاعات در حال انتقال را در بر می گیرد و نسبت به اطلاعات دیگر، شنود همان دسترسی است. محتوای در حال انتقال باید در یك پیوند خصوصی میان دو یا چند نفرانجام گیرد تا شرط انتقال غیرعمومی مفهوم محرمانگی پیدا کند.

در این جرم، رفتار مرتکب شنود یا همان دریافت محتواست. بنابراین میان شنود غیرمجاز و دسترسی غیرمجاز به جهت رفتار تفاوتی وجود ندارد. تفاوت عمده بین این دو جرم در نوع اطلاعات است که مرتکب آن را دریافت می دارد. به این صورت که در دسترسی غیر مجاز، دریافت اطلاعات ذخیره شده و در شنود غیر مجاز دریافت محتوای در حال انتقال انجام می گیرد. همچنین، دسترسی غیر مجاز هم نسبت به اطلاعات است وهم وسایل، ولی شنود غیر مجاز تنها نسبت به اطلاعات رخ می دهد. بنابراین رفتار فیزیکی در این جرم فعل شنیدن می باشد و این جرم با ترك فعل محقق نمی شود.

۳-۴ عنصر روانی جرم

وجود دو مورد بعنوان لازمه تحقق عنصر معنوی در این جرم بحساب می رود. نخست، درک و اگاهی مرتکب از این که چنین تغییر وارد نمودن در سیستم، برنامه یا اطلاعات کمپیوتری غیر مجاز و غیر قانونی می باشد، و دوم اینکه این گونه تغییرات غیر مجاز به اطلاعات، برنامه یا سیستم شخص یا اشخاص دیگر صورت گرفته باشد. یعنی در حریم خصوصی افراد قرار داشته باشد، نه در دسترس همگان. هرگاه محدودیت در استفاده یا تغییر وارد نمودن نسبت به اطلاعات، برنامه یا سیستم ها وجود نداشته باشد، جرم مذبور تحقق نمی یابد.

۳-۵ مؤیدات جزایی جرم

مؤیدات جزائی پیش بینی شده در ماده‌ی ۸۵۳ کود جزای افغانستان عبارت است از حبس متوسط و جزای نقدی از شصت هزار تا سه صد هزار افغانی.

[۱۵] فراهانی، *کنوانسیون جرایم سایبری* ، ۱۶.

۴- از بین بردن غیر مجاز سیستم، برنامه یا اطلاعات کمپیوتری

آسیب رساندن (Damaging) و تخریب (Destruction) به عنوان اعمال هم پوشانیده ای هستند که بطور خاص به تغییر منفی تمامیت یا محتوای اطلاعات، برنامه ها یا سیستم اشاره دارد. حذف (Deletion) اطلاعات معادل از بین بردن یک شی مادی است. این عمل آنها را از بین می برد تا قابل فهم نباشند. متوقف کردن (Suppression) اطلاعات کمپیوتری به معنای هر فعلی است که از دسترس پذیری اطلاعات برای شخصی که به کمپیوتر یا منبع که اطلاعات بر روی آن ذخیره شده و به آنها دسترسی دارد، جلوگیری می کند یا پایان می بخشد. تغییر (Alteration) به معنی دستکاری اطلاعات موجود است. بنابرین وارد کردن کود های مغرضانه، مانند ویروس ها (Viruses) و اسپ های تروا (Trojan Horse) مشمول می گردد، زیرا آنها به تغییر اطلاعات منجر می گردد.[۱۶] مختل کردن (Disruption) به اعمالی بیان می گردد، که در کارکرد نورمال و مناسب سیستم کمپیوتر مداخله می کنند، و این کار با وارد کردن، انتقال دادن، آسیب رساندن، حذف کردن، تغییر دادن یا متوقف کردن اطلاعات کمپیوتری انجام می شود.

۴-۱ عنصر قانونی جرم

عنصر قانونی ضروری وجود جرم در نص قانون است، و مقصود از منابع حقوق جزا نصوص قابل استنادی است که متضمن قاعده ای از قواعد جزائی است، محتوای این قاعده دستور قانونگذار به ادای تکلیف معین و یا نهی از انجام دادن فعلی است که مخل نظم اجتماعی به شمار می رود.[۱۷] بناءً، مادهی ۸۵۴ کود جزای افغانستان بعنوان عنصر قانونی این جرم بحساب می رود.

۴-۲ عنصر مادی جرم

هرگونه تخریب، حذف یا خنثی کردن برنامه، اطلاعات، و سیستم دیگری که منجر به ضرر مادی یا معنوی بر شخص یا اشخاص گردد، عنصر مادی تحقق می گردد. ضمناً، این

---

[۱۶] پیشین، ۳۱.

[۱۷] اردبیلی، *حقوق جزای عمومی*، ۱۳۰.

تخریب، حذف یا خنثی کردن بایست در برابر برنامه، اطلاعات و سیستم دیگری صورت گرفته باشد. بمفهوم اینکه تخریب، حذف یا خنثی سازی در فضای همگانی نباشد. از طرف دیگر مصداق عنصر مادی این جرم می تواند زیر بناهای دولتی، خطوط مواصلاتی زمینی یا هوایی یا وسایل ترانسپورتی یا تأسیسات تولید انرژی یا یکی از تأسیسات حساس دیگر را شامل گردد.

۳-۴ عنصر معنوی جرم

اگاهی و درک از غیر قانونی بودن تخریب، حذف، یا خنثی سازی از یک طرف و بمیان آوردن ضرر مادی و معنوی بعنوان مصداق های تحقق عنصر معنوی بحساب می روند.

۴-۴ مؤیدات جزایی جرم

در صورت‌ی که ازبین بردن غیر مجاز سیستم، برنامه یا اطلاعات کمپیوتری سبب ایجاد ضرر مادی یا معنوی شود، مرتکب حسب ضرر وارده به حبس متوسط یا جزای نقدی از شصت هزار تا سه صدهزار افغانی محکوم به مجازات می گردد. ولی در حالتی که این ازبین بردن های غیر مجاز در برابر زیربناهای دولتی صورت گرفته شده باشد، و سبب ضرر مالی بیش از صد میلیون افغانی گردد، مرتکب به حبس طویل محکوم به مجازات می گردد. و بالاخره، هرگاه از بین بردن های غیر مجاز در برابر خطوط مواصلاتی زمینی یا هوایی یا وسایل ترانسپورتی یا تأسیسات تولید انرژی یا یکی از تأسیسات حساس دیگر صورت گرفته باشد، مرتکب به حبس طویل و در صورتیکه عامل فوت شخصی گردد، مرتکب به حبس دوام درجه ۱ محکوم می گردد.

۵- فریب کاری الکترونیکی

هرگاه شخصی در فضای سایبر با بکار گیری وسایل خدعه آمیز به منظور جلب منفعت به خود یا شخصی دیگر سبب بوجود آمدن خساره به دیگری گردد، جرم فریب کاری الکترونیکی تحقق می یابد.[۱۸]

[۱۸] فتاحی، *بررسی عناصرتشکیل دهنده*، ۱۱۱.

۵-۱ عنصر قانونی جرم

ماده‌ی ۸۵۹ کود جزا عبارت از عنصر قانونی جرم فریب کاری الکترونیکی بحساب می رود.

۵-۲ عنصر مادی جرم

با پیروی از هدایت ماده‌ی ۸۵۹ کود جزا، مصداق های عنصر مادی را بگونه ذیل می توان بیان داشت:

۱. هرگونه دسترسی به سیستم، برنامه یا اطلاعات کمپیوتری که بگونه فریب کارانه جهت کسب منفعت برای خود مرتکب یا دیگری که سبب خساره به دیگری گردد.
۲. هر گونه دخول، تعدیل، تغییر، حذف یا تولید برنامه یا اطلاعات کمپیوتری
۳. مداخله، ممانعت، اخلال یا انسداد عمل کرد سیستم کمپیوتری
۴. کاپی کردن، انتقال یا ارسال اطلاعات یا برنامه به سیستم کمپیوتری، دستگاه یا وسیله ذخیره سازی به استثنای وسیله های که در آن ثبت شده است یا انتقال یا ارسال اطلاعات یا برنامه به موقعیت دیگر در عین سیستم کمپیوتری، دستگاه یا وسیله ذخیره سازی.
۵. استفاده از اطلاعات یا برنامه یا اخراج اطلاعات یا برنامه از سیستم کمپیوتری که در آن ثبت شده است.

باید خاطر نشان کرد که موارد پنج گانه فوق بایست با بکاری وسایل فریب دهنده، جهت حصول منفعت به شخص خود یا شخص دیگری، و ایجاد ضرر به طرف دیگری عاید گردد.

۵-۳ عنصر روانی جرم

عنصر روانی فریب کاری شامل عمد رفتاری یعنی عمد در رفتارهای کمپیوتری تمثیلی و عمد در تحصیل مال یا منفعت می باشد. همچنان، آگاهی مرتکب نسبت به تعلق مال یا منفعت یا خدمات مالی یا امتیازات مالی به شخص دیگر و اینکه انجام رفتارهای کمپیوتری تمثیلی، بدون مجوز بوده است و غیر قانونی می باشد، از جمله عنصر روانی بحساب می رود.

۴-۵ مؤیدات جزایی جرم

قانونگزار کود جزای افغانستان مؤیده جزایی یکسان را بدون پیش بینی کردن حالت مخففه و مشدده در خصوص هر پنج مصداق جرم فریب کاری الکترونیکی در نظر گرفته است. مجازات پیش بینی شده عبارت از جزای حبس متوسط یا جزای نقدی از شصت هزار تا سه صد هزار افغانی می باشد.

٦- جاسوسی سایبری

هرگاه شخصی نسبت به برنامه، اطلاعات یا سیستم کمپیوتری که دارنده یا حامل اطلاعات سری باشد بگونه غیر قانونی دسترسی پیدا نماید، یا در اختیار دیگری قرار دهد، ویا در اختیار دولت، سازمان، شرکت یا گروه خارجی قرار دهد، جاسوسی سایبری تحقق می یابد.[۱۹]

٦-۱ عنصر قانونی جرم

مادهی ٨٦٤ کود جزای افغانستان بعنوان عنصر قانونی این جرم بحساب می رود.

٦-۲ عنصر مادی جرم

قانونگذار در کود جزا، رفتار جرم جاسوسی را در سه گام ذیل پیش بین گردیده است.

۱- دسترسی به اطلاعات سری در حال انتقال یا ذخیره شده در سیستم کمپیوتری یا مخابراتی یا حامل های اطلاعات

۲- در دسترس قرار دادن اطلاعات سری در حال انتقال یا ذخیره شده در سیستم کمپیوتری یا مخابراتی یا حامل های اطلاعات

۳- افشا یا در دسترس قراردادن اطلاعات سری در حال انتقال یا ذخیره شده در سیستم کمپیوتری یا مخابراتی یا حامل اطلاعات برای دولت، سازمان، شرکت یا گروه خارجی یا عاملان آن ها

همین مادهی کود جزای افغانستان اطلاعات سری را به تعریف گرفته و صراحت نموده است که اطلاعات سری عبارت از اسرار مربوط به حاکمیت ملی، تمامیت ارضی یا امنیت ملی

[۱۹] پیشین، ۱۰۱.

کشور می باشد، که در فصل مربوط به جرایم جاسوسی و خیانت ملی، منحیث اسرار دولتی[۲۰] شناخته شده است.

[۲۰] ماده های ۲۳۸ و ۲۴۰ کود جزا به مصداق های خیانت ملی و جاسوسی که به عنوان اسرار دولتی به حساب می رود، به قرار ذیل پرداخته است:

۱. عملی که در نتیجه آن اراضی دولت جمهوری اسلامی افغانستان تماماً یا قسماً تحت حاکمیت دولت خارجی یا نیرو های مسلح مخالف دولت جمهوری اسلامی افغانستان قرار گیرد یا استقلال کشور را به مخاطره اندازد.

۲. عملی که در نتیجه آن تمام یا قسمتی از اراضی تحت حاکمیت دولت جمهوری اسلامی افغانستان از اداره آن خارج شود.

۳. تسلیمی نیروهای تحت امر به دشمن

۴. واگذاری تأسیسات، دیپوی اسلحه و مهمات، وسایل نظامی، ذخایر مواد ارتزاقی یا استحکامات متعلق به نیروهای نظامی به دشمن به منظور مساعدت آن ها، یا فراهم سازی تسهیلات برای ورود دشمن به کشور.

۵. جمع آوری معلومات حاوی اسرار نظامی، دفاعی یا امنیتی کشور، به منظور تسلیم دهی آن به دولت خارجی، سازمان یا گروه ضد دولتی یا گماشتگان آن ها.

٦. استخدام اشخاص، تهیه اموال یا تجهیزات نظامی برای دولت خارجی در حال جنگ با دولت جمهوری اسلامی افغانستان با نیرو های مسلح در حال جنگ یا منازعه مسلحانه با دولت جمهوری اسلامی افغانستان

۷. قیام مسلحانه نیروی های نظامی علیه دولت جمهوری اسلامی افغانستان

۸. سرقت، تلف یا تزویر اسناد حاوی اسرار نظامی، دفاعی یا امنیتی کشور

۹. پیوستن به قوای مسلح دولت خارجی یا گروه مسلح در حال جنگ یا منازعه مسلحانه با جمهوری اسلامی افغانستان

۱۰. قیام مسلحانه با توطئه علیه دولت جمهوری اسلامی افغانستان به منظور گرفتن قدرت دولتی

۱۱. افشای اسرار نظامی، دفاعی یا امنیتی کشور به اشخاص یا دولت خارجی یا شخصی که به نفع آن ها کار می کند، یا به گروه های مسلح مخالف دولت جمهوری اسلامی افغانستان

۱۲. عدم اطلاع از معلوماتی که هدف آن ارتکاب جرایم مندرج اجزای ۱ تا ۸ این ماده بوده و شخص به حکم قانون به کشف آن مؤظف و یا به نحوی دیگری به افشای آن مکلف باشد، به مراجع مسؤول.

۱۳. به همین شکل مصداق های جاسوس

۱۴. تسلیم دهی اسرار نظامی، دفاعی یا امنیتی کشور، به دولت خارجی، سازمان یا گروه ضد دولتی یا گماشتگان آن ها

۱۵. سرقت یا جمع آوری معلومات حاوی اسرار نظامی، دفاعی یا امنیتی کشور به منظور تسلیم دهی آن به دولت خارجی، سازمان یا گروه ضد دولتی یا گماشتگان آن ها

۱٦. جمع آوری یا تسلیم دهی معلومات به دستور اطلاعات و استخبارات دولت خارجی که از آن علیه دولت جمهوری اسلامی افغانستان سؤ استفاده به عمل آمده بتواند.

٦-٣ عنصر روانی جرم

رفتارهای جاسوسی سایبری باید عمداً انجام گیرد چنان که در مادهی ٨٦٤ کود جزا تصریح صورت گرفته است. یعنی موجب به دسترس شدن که طور غیرعمد و از روی بی احتیاطی، بی مبالاتی و یا عدم رعایت تدابیر امنیتی رخ دهد، از حکم ماده مستثنی می باشد. همچنین، مرتکب باید آگاه به سری بودن اطلاعات باشد. نیز طبق بندهای ١ و ٣ مادهی ٨٦٤ کود جزا، مرتکب باید آگاه به غیر صالح بودن فرد یا عامل بیگانه بودن شخص نیز باشد. در نقض تدابیر حامل های موضوع مادهی مذبور نیز باید مرتکب آگاه به این مسأله باشد که وسایل مورد نظر، وسایل‌ای است که اطلاعات سری در آن نگهداری می شوند. در صورت نا آگاهی، جرم دسترسی غیر مجاز موضوع مادهی ٨٥٢ کود جزای افغانستان شکل گرفته است. در انجام رفتارهای جاسوسی نیازی به قصد خاص نیست مگر در نقض تدابیر امنیتی وسایل کمپیوتری یا مخابراتی موضوع مادهی ٨٦٤ کود جزا مرتکب باید قصد دسترسی به اطلاعات سری را داشته باشد.

٦-٤ مؤیدات جزایی جرم

قانونگزار افغانستان مؤیدات جزایی جرایم جاسوسی سایبری را با خیانت ملی و جاسوسی کلاسیک یا سنتی یکی بر شمرده است. در صورتی که مصداق های فقرهی ١ تا ٩ مادهی ٢٣٨ تحقق یابد، مرتکب به حبس دوام درجه ٢ محکوم به مجازات می گردد. ولی هرگاه مصداق های فقرهی ١٠ تا ١٢ مادهی ٢٣٨ تحقق یابد، مرتکب به حبس طویل محکوم به مجازات می گردد. در حالات مشددهی جاسوسی فقرهی ١ تا ١٢، مرتکب به حبس دوام درجه ١ محکوم می گردد.

٧- تروریزم سایبری

همان طور که از این عنوان پیداست، تروریزم سایبری مجموعه ای از اقدامات را شامل می شود که افراد خاصی با نیت خاص مرتکب می شوند و به لحاظ خسارات مادی و لطمات جانی که به بار می آورند، از سوی همه کشورها در زمره شدیدترین جرایم قرار گرفته است.[٢١]

[٢١] فتاحی، بررسی عناصرتشکیل دهنده ، ١٠٨.

۱-۷ عنصر قانونی جرم

مادهی ۸٦۳ کود جزای افغانستان به عنوان عنصر قانونی جرم تروریزم سایبری بشمار رفته چنین بیان می دارد: شخصی که با استفاده از سیستم، برنامه یا اطلاعات کمپیوتری مرتکب جرایم تروریستی این قانون[۲۲] گردد، جرم تروریزم سایبری محقق می گردد.

۲-۷ عنصر مادی جرم

موضوع تروریزم سایبری، وسایل کمپیوتری و مخابراتی که بایست برای ارایه خدمات ضروری عمومی به کار برود، ولی بر علیه دولت جمهوری اسلامی افغانستان، دولت خارجی، سازمان ملی، بین المللی یا هر شخص و نهاد دیگری بمنظور بی ثبات ساختن نظام دولت جمهوری اسلامی افغانستان یا دولت خارجی یا تحت تأثیر قرار دادن سیاست دولت جمهوری اسلامی افغانستان یا دولت خارجی یا سازمان بین المللی انجام یابد، مصداق های جرایم تررویستی سایبری محقق می گردد.

۳-۷ عنصر روانی جرم

مرتکب باید رفتارهای پیش بینی شده در کود جزای افغانستان را از روی عمد انجام دهد. همچنین قصد غایی او به خطر انداختن امنیت، آسایش وامنیت عمومی باشد و از طرف دیگر باید آگاه باشد که رفتار خود را بر روی وسایل که خدمات ضروری ارایه می دهند، انجام می دهد.

۴-۷ مؤیدات جزایی جرم

قانونگزار کود جزا با در نظرداشت حالات مخففه و مشدده از حبس طویل الی اعدام مجازات را برای مرتکبین جرایم تروریستی سایبری در نظر گرفته است.

[۲۲] ماده ۲٦۳ در تعریف جرایم تروریستی صراحت دارد که «ارتکاب اعمال جرمی مندرج این فصل است، به منظور تحت تأثیر قرار دادن سیاست دولت جمهوری اسلامی افغانستان یا دولت خارجی و یا مؤسسه ها و سازمان های ملی یا بین المللی یا بی ثبات ساختن نظام دولت جمهوری اسلامی افغانستان و دولت خارجی».

۸- هرزه نگاری (پورنوگرافی)

هرزه نگاری به مجموعه‌ای از رفتارهای مجرمانه گفته می شود که شامل تولید، طراحی، ارایه، انتشار ومورد معامله قراردادن محتویات شنیداری و دیداری اعم از تصویر، نوشته، و صوت می شود، که عفت عمومی را جریحه دار می سازد.[۲۳] محتویات هرزه شامل محتویات مستهجن و محتویات مبتذل می باشد. آثار مبتذل به آثاری اطلاق می شود که دارای صحنه ها و صور قبیحه باشد در حالی که محتویات مستهجن به تصویر، صوت یا متن واقعی یا غیر واقعی یا متن اطلاق می شود که بیانگر برهنگی کامل زن یا مرد یا اندام تناسلی یا آمیزش یا عمل جنسی انسان باشد.[24]

۸-۱ عنصر قانونی جرم

ماده‌ی ۸۷٤ کود عبارت از عنصر قانونی جرم هرزه نگاری (پورنوگرافی) بحساب می رود. این ماده بیان دارد که شخصی که یکی از اعمال ذیل را انجام دهد، مرتکب جرم پورنوگرافی گردیده است:

۱-تولید پورنوگرافی برای خود یا دیگری یا به منظور نشر در فضای سایبر

۲- پیشکش کردن یا فراهم ساختن پورنوگرافی از طریق فضای سایبر

۳- پخش یا نشر پورنوگرافی در فضای سایبر

۴- نگهداری پورنوگرافی در سیستم کمپیوتری یا در وسیله ذخیره سازی معلومات.

در ادامه ماده‌ی مذکور، وسایل پورنوگرافیکی طوری بیان گردیده است که شخص در حالت عمل جنسی اشکار و تصاویر واقعی نمایش دهنده شخص در حالت عمل جنسی اشکار را قابل رویت می سازد.

---

23 Brain C Lewis, Prevention of Cyber Crime Amidst International Anarchy, *American Criminal Law Review,* 41 (2004), 1355.

24 Susan Brenner, Cybercrime, Cyberterrorism and Cyberwarfare, *International Review of Penal Law*, 77:03-04, (2006), 457.

۲-۸ عنصر مادی جرم

رفتارهای پیش بینی شده در ماده ۸۷٤ کود جزا که مصداق تحقق هرزه نگاری می شوند: تولید، پیشکش یا فراهم نمودن، یا اشاعه و نشر پورنوگرافی در فضای سایبر و یا نگهداری پورنوگرافی در سیستم کمپیوتری یا هر وسیله ذخیره کن دیگر. ولی هرگاه موارد متذکره به قصد تحقیقات علمی، طبی یا حکم قانون صورت گرفته باشد، قابل تعقیب عدلی نمی باشد.

۳-۸ عنصر روانی جرم

برای تحقق جرم هرزه نگاری براساس ماده ۸۷٤ کود جزا لازم است که مرتکب در انجام رفتار گفته شده عمد داشته وهمچنین برای رفتار تولید، پیشکش کردن، پخش و نشر و ذخیره و نگهداری به عمد غایی که در واقع قصد خرید، فروش یا عرضه برای فروش یا عرضه به هر طریق دیگری می باشد، نیز نیاز است. همچنان، اگاهی مرتکب نسبت به رفتار مجرمانه‌ی (مستهجن یا مبتذل) که انجام می دهد ضروری است.

۴-۸ مؤیدات جزایی جرم

قانونگذار افغانستان با در نظر داشت حالات مخففه و مشدده حد اقل مجازات و حداکثر مجازات با ذکر بعضی شرایط مطرح نموده است. شخص‌ی که یکی از اعمال ذکر گردیده را انجام دهد، مرتکب جرم پورنوگرافی بوده، به حبس متوسط تا دوسال یا جزای نقدی از شصت هزار تا یک صد و بیست هزار افغانی محکوم می گردد. هرگاه هدف از پخش و نشر پورنوگرافی، ترغیب طفل به فعالیت های جنسی باشد، مرتکب به حد اکثر مجازات، که دو سال حبس و یک صد و بیست هزار افغانی جزای نقدی می باشد، محکوم می گردد.

چهار مورد ذکر شده در نوت پاورقی در هریک از جرایم سایبری فوق الذکر سبب می گردد، تا حالات مشدده بالای مرتکب اعمال گردد. [۲۵]

---

[۲۵] کود جزای افغانستان در ماده ۸۷٦ در خصوص کلیه جرایم گنجانیده شده در این فصل حالات را تحت عنوان حالات مشدده به قرار ذیل بیان داشته است:

۱- با استفاده از نفوذ، وظیفه یا موقف

۲- به قصد اعمال نفوذ بالای موظف خدمات عامه

۳- با ازبین بردن تدابیر امنیتی مربوط به سیستم کمپیوتری، برنامه یا اطلاعات

نتیجه گیری

با پیشرفت تکنولوژی و استفاده از کمپیوتر در تمام امور اقتصادی، نظامی و اجتماعی جرایم مختلفی می تواند در حوزه سایبر رخ دهد. لذا قانونگذار افغانستان برای مبارزه و پیشگیری از این جرایم در سال ۲۰۱۷ اقدام به تصویب کود جزا نمود، که تا آن دم هیچ گونه قانون وجود نداشت تا جرایم سایبری را جرم انگاری نماید.

البته این دسته از جرایم را می توان شامل جرایم سنتی، که به واسطه کمپیوتر صورت میگیرد از قبیل فریب کاری، سرقت و تروریزم سایبری وغیره، و نیز جرایم نو ظهوری، که با تولد کمپیوتر و پیدایش انترنت پا به عرصه حیات گذاشته اند، مانند جرایم دسترسی غیرمجاز، دانست. یکی از بارزترین کار های تقنینی انجام شده در کود جزای افغانستان تلاش برای تعریف کلیه جرایم سایبری جرم انگاری شده، و یا حد اقل بیان مصداق های جرایم سایبری در این کود می باشد.

قانونگزار کود جزا رفتار های جرمی را در هر گونه جرایم سایبری بگونه جداگانه بیان داشته و مؤیدات جزایی را برای هر یک از رفتار جرمی پیش بینی نموده است. ایراد های را که می توان بیان داشت، در موارد به عوض تعریف جرایم سایبری به بیان مصداق های آن پرداخته است، مثلاً تروریزم سایبری. ولی باید خاطر نشان ساخت که بیان مصداق های یک جرم نمی تواند جاگزین عنصر قانونی جرم بحساب برود. ایراد دیگر در موارد متعدد جایگاه عنصر روانی در تحقق جرایم سایبری خیلی کمتر جلوه داده شده است، بگونه مثال در جاسوسی و تروریزم سایبری. بدین اساس پیشنهاد می گردد، تا باب جرایم سایبری در کود جزای افغانستان بازنگری گردد، و اصلاحات ماهوی و ساختاری در سپهرهای گوناگون آن بوجود آید.

٤- ضررمالی بیش از یک میلیون افغانی وارد نموده یا مرتکب در نتیجه آن عاید مالی بیشتر از میلیون افغانی کسب کرده باشد.