Journal of Socio-Political Developments in Contemporary Iran
Vol. 3, No. 6, spring 2024
http://doi.org/ 10.30510/pscci.2024.488138.1133

Policies, legislative requirements and proportionate punishment of cybercrimes against security in the field of emerging energies with a view to Iran

Sudaba Soleimani[1]
Behzad Razavi Fard[2]
Maryam Safai [3]

Received: 24 January 2023
Reception: 4 June 2024

ABSTRCT
The aim of the present study is to examine the legislative requirements and appropriate punishment of cybercrimes against security in the field of renewable energies with a view to French jurisprudence and law. Cybercrimes have been criminalized as new examples in criminal law in all countries today, but given the nature of these crimes and their history, the criminal policy resulting from these crimes has not yet reached sufficient maturity. The following article examines the legislative requirements and appropriate punishment of cybercrimes against security in the field of renewable energies using a descriptive-analytical method. Iranian criminal laws in this field, from the perspective of accepted principles and the shortcomings and obstacles present in this area, including obstacles in two parts: shortcomings, ambiguities of laws, the effectiveness of the laws in reverse, and the intensification of virtual attacks against renewable energies, can be a new source for punishing and refining criminal laws in the fields of security and cybercrimes against renewable energy infrastructure, and improve the efficiency and preventive role of these laws. On the other hand, the difference between Iranian and French criminal laws in determining crimes against security is due to the influence of jurisprudential and religious teachings in Iran in criminalizing some crimes against security in Iranian criminal law and the lack of this issue in crimes against security in French criminal law. The findings of the research indicate that the formulation of sentencing requirements is like a guideline that is presented to the legislator in the context of punishment, and its correct application leads to the transformation and purposefulness of punishment and the transition from the current situation in energy law to the desired situation in the criminal justice system.

Keywords: Legislative requirements, sentencing, cybercrimes, security, emerging energies,

1 PhD student, Department of Criminal Law and Criminology, Bushehr Branch, Islamic Azad University, Bushehr, Iran

2 Associate Professor, Department of Criminal Law and Criminology, Faculty of Law and Political Sciences, Allameh Tabatabai University, Tehran, Iran.

3Assistant Professor, Department of Law, Bushehr Branch, Islamic Azad University, Bushehr, Iran

فصلنامه تحولات سیاسی اجتماعی معاصر ایران، سال سوم، شماره اول(پیاپی۶)، بهار۱۴۰۳ صص ۲۸۱-۲۶۰
http://doi.org/ 10.30510/pscci.2024.488138.1133

سیاست ها، الزامات تقنینی و کیفرگذاری متناسب جرایم سایبری علیه امنیت در حوزه انرژی های نوپدید با نگاهی به حقوق ایران

سودابه سلیمانی[۱]
بهزاد رضوی فرد[۲]
مریم صفایی[۳]

تاریخ دریافت :۴ /۱۴۰۲/۱۱
تاریخ پذیرش: ۱۴۰۳/۰۳/۱۵

چکیده

هدف پژوهش حاضر، الزامات تقنینی و کیفرگذاری متناسب جرایم سایبری علیه امنیت در حوزه انرژی های نوپدید با نگاهی به فقه و حقوق فرانسه است. جرایم سایبری به عنوان مصادیقی نوین در حقوق کیفری امروزه در تمامی کشورها جرم انگاری گردیده اند، اما با توجه به ماهیت این جرایم و پیشینه آن، سیاست جنایی مترتب بر این جرایم هنوز به بلوغ کافی دست نیافته است. قوانین کیفری ایران در این زمینه از نگاه اصول پذیرفته شده و کاستی ها و موانع حاضر در این گستره از جمله موانع در دو قسمت کاستی ها، اثربخشی واژگونه قوانین و شدت یافتن هجمه های مجازی علیه انرژی های نوپدید می تواند سر منشأ جدیدی برای کیفرگذاری و پیرایش قوانین جزایی در حوزه های امنیتی و جرایم سایبری علیه زیر ساخت های انرژی های نوپدید باشد و نقش پیشگیرانه این قوانین را بهبود بخشد. از طرفی تفاوت میان حقوق جزای ایران و فرانسه در زمینه تعیین جرائم علیه امنیت، ناشی از تأثیر آموزه های فقهی و شرعی در ایران در جرم انگاری بعضی جرائم علیه امنیت در حقوق جزای ایران و فقدان این موضوع در جرائم علیه امنیت در حقوق جزای فرانسه باشد. یافته های تحقیق حاکی از آن است که تدوین بایسته‌های کیفرگذاری، به مانند دستورالعملی می‌ماند که فراروی مقنن در وضع کیفر قرار داشته و کاربست صحیح آن به تحول و هدفمندی کیفر و گذار از وضع موجود در حقوق انرژی به وضع مطلوب در نظام عدالت کیفری می انجامد.

واژگان کلیدی: الزامات تقنینی، امنیت، انرژی های نوپدید، جرایم سایبری، کیفرگذاری.

[۱]دانشجوی دکتری، گروه حقوق جزا و جرم شناسی، واحد بوشهر ، دانشگاه آزاد اسلامی ، بوشهر ، ایران
[۲]دانشیار، گروه حقوق جزا و جرم‌شناسی ، دانشکده حقوق و علوم سیاسی ، دانشگاه علامه طباطبایی ، تهران ، ایران .
[۳]استادیار، گروه حقوق، واحد بوشهر، دانشگاه آزاد اسلامی، بوشهر، ایران

مقدمه

درآمد پیشرفت بی سابقه تکنولوژی در دهه های اخیر باعث تغییرات اساسی در زندگی بشر شده است به گونه ای که رشد فزایندهٔ تکنولوژی، حتّی پدیدآورندگان آن را نیز دچار حیرت کرده است. از مهم ترین نمادهای این پیشرفت، اختراع رایانه می باشد. با ظهور فضای سایبر، تحوّلات وارد مرحلهٔ جدید گردیده است که علاوه بر ارتکاب جرایم سنّتی به شیوه نوین، فضای سایبر نیز بستری برای ارتکاب جرایم مختص به خود به وجود آورده است.جرائم علیه تمامیت و صحت داده ها و اطلاعات نیز از جمله جرائم سایبری محسوب می شود و جرم انگاری این اعمال، این اطمینان را به وجود می آورد که هیچکس بدون داشتن مجوز، حق ندارد به اطلاعات دیگران دست یافته و تغییر در آنها به وجود آورد. قوانین کیفری اگرچه دارای ضمانت اجرایی قوی هستند، اما برای اثربخشی باید تابع قواعد و اصول حقوقی از جمله کارآمدی باشند، زیرا کارآمدی یک قانون، زیربنای انطباق جامعه با آن قانون است. قوانینی که مورد توجه افراد جامعه قرار نمی گیرد، با وجود داشتن ابزار قهریه یا مجازات های شدید، به دلیل ناکارآمدی، با نافرمانی قشر وسیعی از جامعه مواجه می شوند. بررسی اجمالی قوانین کیفری ایران در زمینه جرایم امنیتی حاکی از وجود مشکلات و ابهامات در این زمینه می باشد، اگرچه اعتبار قانون در زمینه جرایم علیه امنیت منوط به پذیرش همگانی یا حداکثری نیست، اما اثربخشی آن مستلزم افزایش ضریب امنیت جامعه می باشد. به سبب اهمیت راهبردی کاربست و راه اندازی سیستم های تولید و توزیع انرژی های نو، سیاست گذاری و تنظیم مقررات در این حوزه جایگاه ویژه ای در میان کشورها دارد. با عنایت به لزوم سیاست گذاری کیفری جهت حمایت از انرژی می توان در سه محور تولید، انتقال و توزیع انرژی این مباحث را مطرح گردد و انرژی به گونه های انرژی نفت و گاز، برق، انرژی بادی و انرژی هسته ای مورد توجه قرار گیرد. با توجه به نیاز سیاست گذاری درست در حمایت کیفری، در کشور ایران نیز قوانین متعددی در زمینه انرژی به تصویب رسیده و تحت عنوان جرایم و مجازات، اعمال و رفتارهایی را جرم انگاری شده است. اثربخشی، کارکرد و اثربخشی قوانین در زمینه جرایم امنیتی در حوزه انرژی های نوظهور از موضوعات چالش برانگیز است که چندان مورد بررسی قرار نگرفته است.

۱- مفهوم شناسی

۱-۱ جرایم علیه امنیت

جرایم علیه امنیت، به عنوان جرایمی با ویژگی‌های متمایزکننده از سایر جرایم از نظر واکنش‌های سختگیرانه مقنن که ناظر بر ارزش‌های مورد حمایت موردنظر آن می‌باشد با مفهوم امنیت ملی پیوندی ناگسستنی دارد و امروزه

تبدیل به بحث روز حقوقی، سیاسی و اجتماعی میان نخبگان و مردم گردیده است. در تعیین معیار، سه نوع ضابطه ذهنی، عینی و شرایط محیطی بیشتر از سایرین مورد توجه علمای حقوق قرار گرفته است(جعفری، ۱۳۹۷: ۷۱) در حوزه جرایم علیه امنیت فضای سایبر در حقوق ایران قانون تجارت الکترونیک از جمله نخستین قوانینی بود که اهمیت فضای سایبری را بر همگان هویدا ساخت. (السان، ۱۳۹۸: ۳۸)

۱-۲ جرم انگاری جرایم سایبری

جرم انگاری نامنظم و گسترده در قوانین جزایی، علاوه بر ایجاد آثار و پیامدهای تورم کیفری، مغایر با اهداف حقوق کیفری نیز می باشد. وجود ضمانت اجراهای خاص در حقوق جزا از قبیل قتل، تحدید آزادی، تنبیه بدنی و... ضرورت جرم انگاری مضیق و اصولی را روشن می کند. جرایم سایبری به دلیل ویژگی هایی مانند سهولت ارتکاب جرم، تعداد زیاد قربانیان و سن پایین اکثر مجرمان، علاوه بر اصول کلی، نیازمند اصول جرم انگاری ویژه نیز هستند.(باستانی، ۱۳۹۰: ۶۵) در کشور ما به موجب قانون جرائم رایانه‌ای مصوب ۱۳۸۸، برای جرائم سایبری جرم انگاری صورت گرفته، اما به صورت صریح، منبع حقوقی در مورد نوع امنیتی آن وجود ندارد.

جرم انگاری در جرایم سایبری زمانی صحیح و قابل قبول است که بر اساس اصولی مانند «ضرورت» و «مشروعیت» انجام شود و ضمن رعایت حریم خصوصی و حقوق شهروندی، تناسب دقیقی بین رفتار مجرمانه و نوع و میزان مجازات داشته باشد. در عین حال به وسایل و ابزارهای موجود نظام عدالت کیفری و گروه های آسیب پذیر توجه شود. بر اساس برآوردی که موسسات بین‌المللی در این خصوص انجام داده‌اند سالانه در حدود ۴۰۰ میلیارد دلار خسارتی است که در ارتباط با جرائم سایبری به کشورها، نهادها و موسسات تحمیل می‌شود.(لله وردی، ۵۴:۱۳۹۶) جرایم سایبری هر فعل یا ترک فعل مجرمانه‌ای که «در»، «از طریق» و یا «به کمک» سیستم های رایانه‌ای رخ می دهد جرم سایبری قلمداد می شود(امیریان فارسانی و دیگران، ۲۳۹:۱۳۹۷) قانونگذار ایران برای مقابله با جرایم سایبری بدون در نظر گرفتن نیاز به تعیین مجازات مناسب، این گونه جرائم را جرم انگاری کرده است که نشان از نگاه تک بعدی به سیاست جنایی ایران دارد (اسکندری، ۱۳۹۷: ۶۷)

۳-۱انرژی های نوپدید

شتاب گرفتن گذار به انرژی های نو در سال های ۲۰۱۲ تا ۲۰۲۲ از طریق افزایش اهمیت انرژی های خورشیدی و باد در تأمین نیازهای انرژی جهان، چشم انداز گسترده ای از تحول در ژئوپلتیک انرژی جهان را ترسیم کرده است.

۱-۳-۱پیدایی و تاریخچه انرژی های نو

پایان پذیری سوخت‌های فسیلی، تنوع منابع انرژی، توسعه پایدار برای ایجاد امنیت انرژی، مشکلات زیست‌محیطی ناشی از استفاده از انرژی‌های فسیلی از یک سو و منابع انرژی تجدیدپذیر مانند خورشید، باد، زیست توده و غیره در از سوی دیگر باعث شده است تا جهان به توسعه و گسترش استفاده از انرژی های تجدیدپذیر و افزایش سهم این منابع در سبد جهانی انرژی توجه جدی داشته باشد. (Zehner,2012: 25).

بر اساس گزارش REN21 سال ۲۰۱۷، انرژی‌های نو در سال ۲۰۱۵ و ۲۰۱۶ به ترتیب ۱۹/۳ درصد در مصرف انرژی جهانی انسان و ۲۴/۵ درصد در تولید برق آن‌ها نقش داشته‌است. این میزان مصرف انرژی به این صورت تقسیم می‌شود: ۸/۹٪ حاصل از زیست‌توده سنتی، ۴/۲٪ از انرژی گرمایی (زیست‌توده مدرن، زمین‌گرمایی و گرمای خورشیدی)، ۳/۹٪ حاصل از برق آبی و ۲/۲٪ باقیمانده برق حاصل از باد، خورشید، زمین‌گرمایی و دیگر اشکال زیست‌توده است. اتانول زیستی و بیودیزل سوختی که از محصولاتی مانند ذرت، نیشکر، کنف و کاساوا تهیه می‌شود. انرژی های تجدیدپذیر حدود ۲۰ درصد از کل برق ایالات متحده را تولید می کند و این درصد همچنان در حال رشد است. علاوه بر این کشورهای پیشرو در بهره‌مندی از انرژی‌های تجدیدپذیر و نو در بسیاری از کشورها چون مالزی، ژاپن، مراکش، نیوزلند،چین، آلمان و نروژ می باشند(Jupe,2017:51). در ایران شیخ بهایی، با استفاده از انرژی زیست توده (بیومس) کوره مشهور در حمام موسوم به شیخ بهایی را گرم می ساخته است. این کوره تنها با یک شمع، آب حمام را گرم می کرد. در سال های اخیر نگرانی های در خصوص افزایش مصرف انرژی و کاهش منابع سوخت های فسیلی بیشتر شده است. بنابراین، روز به روز علاقه به منابع تجدیدپذیر در ریز شبکه ها بدلیل هزینه پایین و راندمان بالا بیشتر شده است. سیستم های توزیع dc مانند سلول های خورشیدی و پیل سوختی مورد توجه قرار گرفته اند.(امینی زارع، ۱۳۹۲: ۵۴)

۱-۳-۲ انرژی زیست سوخت ها

زیست سوخت‌ها شامل دامنه گسترده‌ای از سوخت‌ها است که از زیست‌توده حاصل می‌شوند. این اصطلاح سوخت جامد، مایع و گاز را در بر می‌گیرد.(Jupe,2017:32). سوخت‌های زیستی مایع شامل الکل‌های زیستی مانند بیواتانول و روغن‌هایی مانند بیودیزل است. سوخت‌های زیستی گازی شامل بیوگاز، گاز محل دفن و گاز مصنوعی است. بیواتانول الکلی است که با تخمیر اجزای قند مواد گیاهی تهیه می‌شود و بیشتر از محصولات شکر و نشاسته تهیه می‌شود.(Wasielewski , Styring,2019:87)

۱-۳-۳ انرژی های خورشیدی

نور تابشی و انرژی گرمایی خورشید با استفاده از کلکتورهای خورشیدی مهار می شـــود. این کلکتورهای خورشـــیدی انواع مختلفی دارند مانند فتوولتائیک، فتوولتائیک متمرکز، گرمایش خورشـیدی، نیروی خورشـیدی متمرکز (CSP)، فتوسنتز مصنوعی و معماری خورشیدی. این انرژی خورشیدی جمع‌آوری‌شده سپس برای تأمین نور، گرما و دیگر اشکال برق استفاده می‌شود.

۱-۳-۴ انرژی بادی

انرژی بادی به عنوان یکی از انواع انرژی های نو از طریق نصـــب توربین های بادی در نواحی ساحلی، کوهستانی و همچنین دشت ها به تولید می رسد. این توربین ها با بهره برداری از انرژی جنبشـــی حاصـــل از باد و تبدیل آن به الکتریسیته، منبعی برای تولید جریان برق محسوب می شوند.

۱-۳-۵ انرژی زمین گرمایی

انرژی زمین گرمایی یکی دیگر از انواع انرژی های نو اســـت که از حرارت تجمع یـافتـه در بخش زیرین ســـطح کره زمین اســـتفـاده می کنـد. همچنین تکنولوژی اســتخراج و بهره برداری انرژی زمین گرمایی به عنوان یکی از انواع انرژی های نو، مشابه فناوری به کار رفته در صنعت نفت می باشد.

۱-۳-۶ انرژی آبی

انرژی آبی که به عنوان نیروی برق آبی نیز شـــناخته می شـــود، یک منبع انرژی تجدیدپذیر اســت که با اســتفاده از نیروی آب در حال حرکت باعث چرخاندن توربین آبی و ســـپس تولید برق می شـــود. انرژی آبی معمولا در نیروگاه های برق آبی در مقیاس بزرگ که در نزدیکی رودخانه ها، آبشارها یا سایر منابع آب متحرک قرار دارند، تولید می شود.

۱-۴تروریسم انرژی

جرایم ســـایبری به عنوان مصـــادیقی نوین در حقوق کیفری امروزه در تمامی کشورها جرم انگاری گردیده اند، اما با توجه به ماهیت این جرایم و پیشینه آن، سـیاسـت جنایی مترتب بر این جرایم هنوز به بلوغ کافی دسـت نیافته اسـت.(آقابابایی، ۴۶:۱۳۸۹). با ظهور تکنولوژی رایانه و اینترنت، این ابزار در خدمت مجرمین قرارگرفته و در جرائم امنیتی به عنوان ابزاری برای ارتکاب جرم یا به عنوان هدف جرم تلقی می‌شود. در سال ۲۰۱۰، استاکس نت به دلیل عملکرد و پیچیدگی آن مورد توجه کارشـناسـان قرار گرفت. این بدافزار برای هدف قرار دادن کامپیوترهای خاصـی در ایران طراحی شـده اسـت. اگرچه اسـتاکس نت از طریق اینترنت در ســراســر جهان گســترش یافته اســت، اما اثرات مخرب آن محدود به سیستم های کنترلی خاص در ایران بوده است. با رمزگشایی کدهای این بدافزار مشـخص شـد که به عنوان سـلاحی علیه تاسـیسـات هسـته ای

کشورمان برای ایجاد اختلال در عملیات گازی سازی سانتریفیوژها در فرآیند غنی سازی طراحی و به کار گرفته شده است. اهداف و اثرات این بدافزار به میزانی بود که شمار زیادی آن را با یک حمله مسلحانه قیاس نمودند. (پاکزاد، ۴۳۲:۱۳۹).

۳- سیاست گذاری تقنینی و جلوه های سایبری انرژی های نو پدید

پایه‌های اصلی سیاست جنایی ایران در قبال جرایم سایبری حوزه انرژی را نامتغیرها- روابط اصلی و روابط تکمیلی تشکیل می‌دهد. منظور ما از نامتغیرها در سیاست جنایی همان پدیده جنایی (بره و انحراف) و پاسخ های هیأت اجتماع (پاسخ های دولت و پاسخ های جامعه مدنی) است. قانون انرژی و جرایم پیرامونی آن با پیچیدگی مزمن مواجه است وضعیت حقوقی و رژیم انرژی فاقد وحدت است. تضمین منابع انرژی نیاز به بهره‌گیری از ظرفیت‌های حقوقی دارد که راهبردهای نوین سیاست‌جنایی با طیف وسیعی از ابزارهای کیفری و غیرکیفری در قالب سیاست کیفری، حمایتی، پیشگیرانه و مشارکتی ظرفیت مناسبی برای حمایت از انرژی دارد. سیاست‌جنایی ایران در قبال انرژی عملتاً مبتنی بر الگوی «سیاست جنایی دولتی» است که دولت را محور تصمیم‌سازی و اقدام‌ها دانسته و رویکرد «فرمان-کنترل» را در مسائل انرژی به عنوان خط‌مشی پذیرفته است(اله‌وردی، ۳۷:۱۳۹۶) .

در حوزه تقنینی انرژی و به خصوص انرژی های نو پدید ضعف های جدی در زمینه های گوناگون حقوقی و الزامات فنی و مدیریتی، سبب می شود که مقنن برای وضع قانون متناسب که به طور سنتی در حوزه صلاحیت انحصاری شان قرار داشته است، با محدودیت های قابل توجهی رو به رو شوند و ضرورت توسل به بخش خصوصی فنی محور در حوزه انرژی و به ویژه اشخاص حقوقی ملی و فراملی و بهره مند از توانمندی های گوناگون سایبری، که وضع قوانین این حوزه را را تبدیل به قانونی کارآمد و پربازده می کند، بیش از پیش خودنمایی کند.(ارشدی و همکاران، ۱۴۰۰: ۸۳)

ماهیت گسترده و گستردگی جهانی فضای سایبری زمینه را برای ایجاد تهدیدات سایبری در ابعاد سیاسی، اقتصادی، اجتماعی، فرهنگی، زیست محیطی و دفاعی-نظامی فراهم نموده است .تهدیدات سایبری در حوزه نظامی و دفاعی بر خلاف ابعاد دیگر، رویکردی سخت و چهره ای خشن دارد. بسیاری از این تهدیدها احتمالاً به سبب محدودیت های بین المللی وجود دارند و فقط جنبه بازدارندگی دارند. در صورت افزایش تنش و درگیری بین کشورها، این تهدیدها به مرحله عملیات و جنگ می انجامد. در یک دسته بندی کلی، ویژگی های تهدیدات سایبری را می توان شامل موارد زیر دانست:

۱) منبع تهدید: مزدوران سایبری یا گروه های مخفی تحت حمایت دولت، دولت های متخاصم، تروریست های سایبری، جاسوسان سایبری، مجرمان سایبری سازمان یافته، هکرهای با انگیزه سیاسی.

۲) پیامدهای تهدید: خطر سایبری (احتمال سوء استفاده از یک تهدید سایبری از آسیب پذیری سایبری در یک پایتخت سایبری) و حمله سایبری (اقدام عملی تهدید سوء استفاده از آسیب پذیری سایبری)

۳) سطح تهدید: زیرساختی، سازمانی، ملی و فراملی.

۴) احتمال وقوع تهدید: احتمال اینکه یک تهدید از آسیب پذیری برای ایجاد یک خطر سایبری سوء استفاده کند.

۵) شدت تهدید: شدت بسیارکم (تهدیدی که منجر به آسیب محدود و قابل کنترل می شود)، شدت پایین (تهدید سایبری که باعث حادثه می شود)، شدت متوسط (تهدیدی که منجر به یک حادثه امنیتی می شود) و شدت بالا (سایبری در مقیاس بزرگ). بحران ها و زیان هایی مانند اختلال در اینترنت) بانکداری شبکه ای)، بیش از حد (تهدیدهای فاجعه بار مانند خرابی شبکه سراسری برق) (هلیلی، ۱۴۰۰: ۱۰۲)

در بحث جرایم سایبری در حوزه انرژی های نو و تجدیدپذیر که عمدۀ تخریب‌ها به صورت غیرقراردادی صورت می‌گیرد، قابل پیش‌بینی بودن ضرر چندان کاربردی ندارد و ادعای این‌که قابل پیش‌بینی بودن ضرر در مسئولیت قراردادی و غیرقراردادی به طور یکسان اجرا می شود، به سادگی قابل اثبات نیست. در حقوق ایران این شرط را می‌توان از مادۀ ۵۲۱ق.م.ا. مصوب ۱۳۹۲. استنباط نمود.

این شرط را از سخن برخی از فقها نیز می‌توان استفاده کرد. مرحوم محقق کرکی در بحث تلف می‌گوید: «اذا کان‌العامل مما کان یتوقع معه علۀ التلف بان یکون جودها معه کثیراً (محقق داماد، ۱۴۰۰: ۱۳۴) اما در رابطه با جرایم سایبری در حوزه انرژی های تجدیدپذیر و تعدد عاملان خسارت هنوز بسترهای مناسبی برای اجرای این گونه مسئولیت در نظام حقوقی کشور ایران ایجاد نشده است با تبیین مسئولیت‌های تقسیم ناپذیر و تفکیک آن از انواع مسئولیت‌ها و ایجاد راهکار در زمان تعدد فاعلان فعل زیانبار، به وسیله‌ی قانون گذار و دکترین حقوقی و با استفاده از انعطاف نظام حقوقی ایران در برابر مسئولیت‌های مدنی و جبران خسارت، برای ایجاد یک دیدگاه جدید در مسئولیت‌های تقسیم ناپذیر، می‌توان چنین سیستم مسئولیتی را در نظام حقوقی ایران تضمین کرد. یکی دیگر از نظریاتی که در آراء اندیشمندان حقوقی غربی و متأثر از نظریات جدید مسؤولیت در قرن بیستم مطرح شده، تئوری «رابطه سببیت نسبی» است. با استفاده از سببیت نسبی، میتوانیم مفاهیم مسئولیت بدون

تقصیر مثل مسئولیت ناشی از تولید و فعالیتهای خطرناک جرایم سایبری در حوزه انرژی های نو را برای پوشش دادن حوزه های وسیع تری توسعه دهیم. با استفاده از قسمت اخیر ماده ۶۲۵ قانون مجازات اسلامی ۱۳۹۲، می توان گفت نظریه سببیت نسبی در حقوق کشور ما نیز مورد پذیرش قرار گرفته و قانونگذار به تأثیر نسبی پرداخته است نه تقصیر نسبی.

ایران نیز در حوزه انرژی های نوپدید یکی از کشورهایی است که در معرض پدیده «تروریسم» و «تروریسم سایبری» قرار دارد. با توجه به این شرایط، ایران باید بیش از هر کشور و هر دولتی از مقابله و مبارزه با تروریسم در پرتو ایدئولوژی های اسلامی و انسان دوستانه خود در بستر پدیده «تروریسم» و در راستای تحقق اهداف سیاسی بشردوستانه بهره مند شود. "تروریسم" و کار برای مقابله با آن باید با هدف ایجاد سازوکار و کار داخلی برای مقابله با تروریسم باشد، در واقع سیاست های ایران در مبارزه با تروریسم با هدف امنیت ملی، پیشگیری و کنترل (دراز مدت) از این پدیده و پدیده تروریسم به صورت تاکتیکی و نظامی (کوتاه مدت) و برخورد قانونی با تروریسم سایبری. (جعفری، ۱۳۹۷: ۴۵) از آنجایی که ایران از نظر نظامی در موقعیت مناسبی برای برقراری امنیت مرزی و دفاعی کشور قرار دارد، توجه دشمنان و تروریسم به فناوری اطلاعات در حوزه نیروگاه های آبی و پنل های خورشیدی است و ایران نیازمند اتخاذ تدابیر امنیتی برای تضمین این امر است(محبی و ریاضت، ۲۹:۱۳۹۵).

۱-۳سابوتاژ کامپیوتری در حوزه انرژی نوپدید

اصلاح ساختار اقتصادی صنایع تحت مقررات و موانع اصلاح ساختار آنها از جمله انرژی نوپدید موضوع مهمی است. در همه کشورها از جمله ایران به دلیل حساسیت زیاد انرژی نوپدید و لزوم پیوستگی عرصه انرژی، اصلاح مناسب ساختار بخش های مختلف صنعت انرژی از جمله بخش توزیع اهمیت زیادی دارد. شبکه های انتقال برق به سبب وابستگی به فضای مجازی و اینترنت یکی از مهم ترین مقاصد جنگ مجازی به شمار می آیند. در سال ۲۰۰۹. دولت ایالات متحده بیان داشت که دولت های چین و روسیه قصد دارند با نفوذ به نرم افزار، شبکه برق کشور را مختل نمایند. از سوی دیگر و بالعکس، حملات نظامی علیه شبکه های انتقال برق جهت کار انداختن اینترنت از جمله موارد نگران کننده جنگ مجازی می باشد.

با تغییر ایدئولوژی حاکم بر کشـــور و همچنین شـــدت و کاهش عملیات خرابکارانه علیه تاســـیســـات عمومی و زیربنایی، اقدامات قانونگذار نیز برای مقابله با آن، دچار افت و خیز شده است. این موضوع موجب گردیده است تا در قواعد و سازوکارهای کیفری برای مقابله با تروریسم مادی ابهامات و حتی در مواردی تعارض بروز داده شود. (ارشدی و همکاران، ۱۴۰۰: ۴۳)

۳-۲ اخلال و خرابکاری در صنایع تولیدی منشأ از انرژی نوپدید

خرابکاری سایبری عنوان مجموعه ای از جرایم رایانه ای است که علیه تمامیت داده و سامانه های رایانه ای صورت می گیرند و در فضای سایبر خسارات فراوانی ایجاد می کنند. ارزش تمامیت داده و سامانه های رایانه ای یکی از مهم ترین اصول امنیت رایانه به شمار می آید که به حفظ موجودیت و یکپارچگی داده ها و ســـاملنه های رلیلنه ای اشـــاره دارد. قانون جرایم رلیلنه ای ایران در جهت حمایت از این ارزش، موادی را به جرم انگاری جرایم علیه تمامیت داده و سامانه های رایانه ای اختصاص داده اس(شریفی خضارتی، ۶۵:۱۳۹۸).

از سوی دیگر، به فعالیت های نظامی که با استفاده از ماهواره و رایانه، تجهیزات دشـــمن را مختل می کند، خرابکاری می گویند. زیرســـاخت های برق، آب، سوخت، ارتباطات، حمل و نقل و غیره ممکن است در جنگ مجازی در خطر باشد. این شامل اختلال در سرورهای وب، سیستم‌های اطلاعات سازمانی، سیستم‌های سرور، لینک‌های ارتباطی، تجهیزات شبکه و رایانه‌های رومیزی و لپ‌تاپ‌های خانگی و امور تجاری می‌شـــود که گاهی برای کســـب انگیزه‌های رقابتی یا مالی و گاهی خرابکاری به دلیل صرفاً سرگرمی انجام می‌شود.

از این رو می توان اشاره داشت به ماده ۲ قانون مجازات اخلالگران در سیستم اقتصـــادی کشـــور برای جرم اخلال کلان و عمده در نظام اقتصـــادی کشـــور، مجازات اعدام را در صورتی‌که جرم باانگیزه مقابله با نظام جمهوری اسلامی یا تعرض به آن یا اطلاع از اثربخشـــی اقدام علیه نظام مذکور در شـــرایطی که در حد افســـاد فی الارض باشـــد، عامل این جنایت را مشـــخص نموده اســـت. با تصویب ماده ۲۸۶ قانون مجازات اسلامی در سال ۱۳۹۲ و اراده قانونگذار مبنی بر اینکه جرم افساد فی الارض جزء جرایم مشمول حد محسوب می گردد، اخلال در نظام اقتصادی نیز از مصادیق ذکر شده است. در این ماده که در صورت احراز شرایط مقرر در ماده مشمول مجازات افساد است. روی زمین خواهد بود.

۳-۳دستیابی غیرمجاز و محرمانگی داده های الکترونیکی

با توجه به اهمیت محرمانگی داده های الکترونیکی و جرایمی که در ســـراســـر جهان در مورد آن رخ می دهد که امنیت و منافع کشورها را به طور عام و افراد را به طور خاص تهدید می کند و خطر آن را به دلیل ارتکاب کامپیوتری

افزایش داده است. در جاسوسی امنیتی، افشا و دسترسی غیرمجاز به اسناد سری و محرمانه، صـدمه جدی به منافع عمومی و امنیت کشـور وارد می‌سـازد. در حوزه انرژی نو پدید در جاسـوسـی صـنعتی نیز دسـتیابی غیرمجاز به اسـرار تجاری و اقتصادی یک کشور، منجر به در خطر افتادن دادوستد افراد با یکدیگر و یا ازبین رفتن اموال و خدمات آنها می‌شـود، که در صـورت برهم‌زدن امنیت انرژی کشور، خود نوعی جاسوسی امنیتی تلقی می‌شود. جاسوسی سایبری به عمل به دست آوردن اسرار (اطلاعات حساس، اختصاصی یا طبقه بندی شده) از افراد، رقبا، گروه ها، دولت ها و دشـمنان برای اسـتفاده نظامی، سـیاسـی یا اقتصادی با استفاده از روش های بهره برداری غیرقانونی از طریق اینترنت اشاره دارد(حبیب‌زاده، ۵۴:۱۴۰۰).

۴-الزامات ایجابی و ساختاری تقنینی بالادستی

۴-۱ قوانین ملی و محلی

قانونگذاران ملی و همچنین نهاد های بین المللی مانند آژانس بین المللی انرژی و آژانس بین المللی انرژی های تجدیدپذیر و UNFCC تلاش های قابل توجهی در زمینه مساعد کردن شرایط گذار انجام داده اند و بسیاری از کشورها قوانین سختگیرانه و اهداف مشخصی (تا سال ۲۰۳۰ و ۲۰۵۰) تعیین کرده اند؛ در حالی که جمهوری اسـلامی ایران اهداف و راهکار مشـخصـی در این خصـوص ارئه نکرده اسـت. کشـورها با روش های مختلف کنترل پدیده تروریسـم در جهت تامین امنیت ملی و حفظ حاکمیت در صـدد پیشـگیری و کنترل و مبارزه با این پدیده می باشـند. متاسـفانه ناکارآمدی سـیسـتم عدالت کیفری بین المللی نیز باعث رشد روزافزون این جرم گردیده است. با توجه به اهمیت این پدیده مخصوصا در دهه های اخیر به تدریج توجه جرم شناسان به شـکل نوین و خطرناکی از پدیده مجرمانه جلب گردیدکه با ویژگی هایی چون فراملی و سـازمانی بودن آمیخته بود. در اکثر اسـناد بین المللی این عنوان همراه با عنوان پولشویی ذکر شده است، زیرا کارشناسان معتقدند شباهت زیادی بین این دو عنوان وجود دارد. این رویکرد تا زمانی مؤثر بود که بیشتر منابع مالی از حمایت مالی ثروتمندان و دولت ها تأمین می شـد، اما امروزه با تغییرات درون گروه های تروریستی، مقابله با منابع مالی تروریست ها با تدابیر اتخاذ شده در امور امکان پذیر نیست. از پولشـویی امروزه گروه های تروریستی بیشتر منابع مالی خود را از سـرزمین های اشـغالی، تجارت و جرایم سـازمان یافته تامین می کنند (بوگانسکی، پترسکی، ۱۳۹۴: ۲۵۲).

فقدان قوانین بین المللی باعث شـده اسـت که هر کشـوری وارد جنگ مجازی علیه کشـور دیگری گردد. در حال حاضـر آمریکا در دنیا یک مرکز فرماندهی فضـای سـایبری در پنتاگون ایجاد نموده است که هدف آن حمله به شـبکه های

دیگر کشـــورها و دفاع در مقابل حملات ســـایبری می باشـــد. آژانس امنیت اطلاعات و شـبکه‌ی اروپا نیز چنین مرکزی به شـمار می آید. به عبارت دیگر، امروز جهان با اقتصـــاد تروریســـم مواجه اســـت. بر این اســـاس برای طراحی سیستمی موثر برای مقابله با تامین مالی تروریسم، علاوه بر استفاده از اقدامات مبارزه با پولشـــویی، باید به اقدامات توصـیه شـده در اسـناد مربوط به جرایم ســـازمان یافته نیز توجه کرد. مقابله با تامین مالی تروریســـم در حوزه انرژی بخشی از تلاش جامع تر جامعه بین المللی برای مقابله با تروریسم است.

۴-۲ سیاست های توسعه امنیت ساختاری و فنی

در بیشـتر کشـورها تا قبل از دهه ۱۹۸۰، حوزه سـیاسـت‌گذاری صـرفاً از طریق دولت و امور مربوط به تصدی‌گری بسته به ماهیت موضوع یا توسط دولت (در قالب شـرکت‌های دولتی) و یا توسـط بخش خصـوصـی انجام می‌شـد. در اوایل این دهه، به تدریج با آشـــکار شـــدن ناکارآمدی‌های دولت‌ها در عرصـــه تصـــدی‌گری به ویژه فعالیت در حوزه صـــنایع شـــبکه‌ای نظیر برق، گاز و مخابرات، بـه تـدریج زمینـه واگـذاری اینگونـه فعـالیـت‌هـا از دولـت بـه بخش خصـــوصـــی مطرح شـــد(کتانچی؛ بابک، ۳۲:۱۳۹۸). جرائم موجود در فضـــای ســـایبری از زمره جرائم با ویژگی‌های خاص و پیچیده محســـوب می‌گردند. در رابطه با ای جرائم دو دیدگاهِ لزوم مواجه افتراقی و عدم لزوم آن مطرح اســـت. مهمترین شـــان عبارتند از: افزایش قدرت تشـــخیص و تجزیه و تحلیل و نیز آشکار شدن نقش فناوری مدرن و توانایش در شناسایی هر چه سریعتر و دقیق تر فعالیت های متقلبانه و حملات سـایبری ، پیشـرفت سـیسـتم های امنیتی و فناوری مدرن که به توسعه ی امنیت و کارکرد سیستم های حفاظت الکترونیکی کمک می کند ، آگاهی و آموزش، از آنجایی که فناوری روز نقش مهمی در افزایش آگاهی و آموزش کاربران در مورد خطرات جرایم سایبری ایفا می کند، از طریق روش های آگاهی الکترونیکی و منابع آموزشـــی، دانش و اطلاعات زیـادی در مورد امنیـت دیجیتـال و اقـدامـات ایمن در اینترنـت منتشـــر می شود(حاجی رضایی، ۳۶:۱۴۰۰).

۴-۳ ضرورت انتقال تکنولوژی در بستر حقوق

توجه به ویژگی های و تمایزات بزه های فضـای مجازی در مقایسـه با بزه های ارتکابیِ دنیایِ واقعی، این امر را قابل درک می سـازد که الگوهای ارتکاب جرم در این فضـا با الگوهای جرایم سـنتی تمایزات قابل توجهی دارند؛ و به واسـطه ی این تحولات و تمایزات و عدم کارایی نظام کیفری سـنتی در مقابله با جرایم سـایبری است که تبیین رویکرد افتراقی را در قلمرو جرایم سـایبر، ضـروری می نماید. رویکرد جنایی سـنتی موجود و مرسـوم مربوط به زمانی است که فناوری در مراحل اولیه خود بود. اما امروزه رشـد و توسـعه فناوری امکان اسـتفاده از

نیروهای سازمان یافته انسانی و منابع و امکلنات متمرکز را برای مقابله با مجرمان در فضای سایبری محدود کرده است. به نظر می رسد تحولات ناشی از پیدایش فضای سایبر، متمایز از دگرگونی هایی است که در اثر گسترش دیگر فناوریهای پیچیده و مدرن پدیدار شده است(ملکیان، ۱۳۹۵: ۱۳۷)

اتوماسیون در سیستم‌های توزیع با پیشرفت تکنولوژی و پیدایش تولیدات پراکنده شکل گرفت. تخمین حالت از توابع پایه‌ای برای اتوماسیون و نظارت بر سیستم‌های توزیع به شمار می‌رود. با کمک تخمین حالت سیستم‌های توزیع، اپراتور می‌تواند به عملکردی امن، اقتصادی و بهینه‌تر از سیستم توزیع دست یابد.(سلطانی، ۱۳۹۳: ۳۹)

برای توسعه تکنولوژی و بازار انرژی‌های نو، توسعه سیاست های ملی و محلی در زمینه پتانسیل سنجی و شناسایی منابع، ساخت، نصب و بهره برداری از انرژی‌های تجدیدپذیر الزامی است. همچنین، برای بهره‌برداری مناسب و هوشمند از منابع فسیلی نیازمند تبیین و آسیب‌شناسی توسعه‌نیافتگی این منابع، به همراه شناخت پتانسیل های موجود و ایجاد ساختارهای مقتضی و حمایت قاطع از این ساختارها است(دبیر نیا، ۵۴:۱۳۹۸). در ایران به غیر از قانون خرید تضمینی برق از منابع تجدیدپذیر، قانون حمایتی و راهبری برای توسعه استفاده از انرژی های نو وجود ندارد، بنابراین لازم است راهبردها و برنامه ریزی های اساسی در این زمینه تدوین گردد. همچنین لازم است سازمان انرژی های نو ایران به عنوان متولی توسعه این بخش از انرژی کشور، قوانین ملی و محلی را در خصوص حقوق مالکیت و بهره برداری از منابع، چگونگی و اصول بهره برداری در راستای توسعه پایدار منابع و توسعه دانش فنی تدوین کند.

۵-کیفرگذاری متناسب

۵-۱ جرم‌انگاری فرا ضابطه ای و فراگیر

جرم‌انگاری فرا ضابطه ای و فراگیر در قوانین کیفری علاوه بر اینکه سبب ایجاد آثار و تبعات منفی انباشت کیفری را فراهم می سازد با اغراض حقوق کیفری نیز در تغایر است. با وجود ضمانت اجراهایی ویژه در حقوق کیفری مانند سلب حیات، تحدید آزادی، مجازات جسمانی و ... ضرورت جرم‌انگاری محدود و بر پایه مبانی را به خوبی هویدا می‌سازد.سازمان های تروریستی برای اینکه بتوانند اعمال تروریستی را ادامه دهند، متوسل به کمک مالی از دیگران می شوند. برای جلوگیری از تأمین مالی تروریسم، کشورهای گوناگون برای کسانی که منابع مالی تروریست ها را تأمین کنند، مجازات تعیین نموده است. قانون ضد تروریسم ۲۰۰۸ انگلستان که حاوی مقرراتی است که به تأمین مالی تروریسم اختصاص داده شده است، نمونه ای از قانون گذاری در این موضوع است(هریسن داینیس، ۳۹:۱۳۹۵). به منظور تدوین سیاست جنایی کارآمد در

جرایم سایبری در حوزه انرژی های نو، باید اقدامات پیشگیرلنه و کیفری مناسب با تمرکز بر ماهیت این جرم و نه صرفاً روش ها اتخاذ شود. در مواجهه با جهانی شدن حقوق کیفری، نظام حقوقی ایران بیشترین همگرایی را در زمینه مسائل اقتصادی داشته است. بر این اساس، تامین مالی تروریسم مانند پولشویی به یکی از موضوعات حقوق کیفری ایران تبدیل شده است.

لازم به ذکر است قانون مبارزه با تامین مالی تروریسم پس از اصلاحات متعدد در مجلس در تاریخ ۱۳۹۴/۱۲/۱۳در نهایت به تصویب شورای نگهبان رسید، اما ایران هنوز به کنوانسیون بین المللی مقابله با تامین مالی تروریسم نپیوسته است. الحاق ایران به ۶ کنوانسیون از ۱۳ کنوانسیون بین المللی مبارزه با تروریسم و عدم التزام به کنوانسیون مذکور و انطباق ناقص قانون مبارزه با تامین مالی تروریسم از اقدامات و تعهدات مورد نیاز اسناد بین المللی و همچنین عدم انطباق مستقل قانون مبارزه با تامین مالی تروریسم.

مقابله با تامین مالی تروریسم بخشی از سیاست جنایی مقابله با تروریسم است، بنابراین با توجه به عناوین کیفری فعلی قانون جزایی ایران، رسیدگی به تمامی موارد تروریسم امکان پذیر نیست. بر این اساس، جرم انگاری تامین مالی تروریسم در جمهوری اسلامی ایران بدون ایجاد سازوکارهای قانونی دیگر برای مقابله با تروریسم راه حل کافی برای مقابله با آن است مشکلی نیست. (تبریزی و همکاران، ۱۴۰۱: ۹۱)

۵-۲ ارزیابی دلایل جرایم امنیتی سایبری و پیشگیری از آن

۱-زمینه سنجی

جرائم امنیتی سایبری به دلایل مختلف ارتکاب می‌یابد که مهمترین آن‌ها دلایل سیاسی، نظامی، اقتصادی، فرهنگی، اجتماعی، روحی و روانی هستند. از دیدگاه حقوقی نیز به خلأ قانون‌گذاری در این حوزه، نبود ضمانت‌های لازم برای عدم تکرار این جرائم و بازدارنده نبودن برخی مجازاتهای قانونی اشاره شده و لزوم قطع زنجیره آموزش این توانایی‌ها توصیه گردیده است. پیشگیری از وقوع این جرائم در دو جنبه کیفری و غیرکیفری مدنظر است که همکاری نهادهای مختلف در این حوزه را نیازمند است. قوه مجریه به نوبه خود وظیفه ثبات وضعیت کشور از هر نظر را عهده‌دار بوده تا دلایل وقوع چنین جرائمی از بین رود(محبی و ریاضت، ۱۳۹۵: ۲۱)

۲-بایسته های تقنینی

قوه مقننه نیز با توجه به وظیفه قانون‌گذاری خود، ملزم به مرتفع کردن خلأهای تقنینی در این حوزه است و قوه قضائیه در بخش پیشگیری و دادرسی این جرائم مسئولیت‌هایی دارد. با وجود تصویب قانون پیشگیری از جرم در سال ۱۳۹۰، اما الزام به همکاری و هماهنگی نهادهای مستقل که در مسئله جرائم

امنیتی دخیل هستند، تامین نشده و به کلی بودن این قانون انتقادهایی وارد است. از طرفی نیز سیاست تقنینی جرایم سایبری ناظر به تدابیر پیشگیرانه جرایم سایبری در حوزه انرژی شامل گسترش ایمنی سامانه های داخلی، به کار گیری نیروهای معتمد، متعهد و متخصص و تدوین قوانین شفاف و سختگیرانه برای حوزۀ سایبر نیست(انصاری، ۳۲:۱۳۹۶). از سویی در گستره بین المللی نیز همکاری آن‌ها برای تدوین یک معاهدۀ بین المللی الزام‌آور دربارۀ ممنوعیت حملات سایبری به بخش انرژی، می تولند مهم ترین اقدام می تولند قلمداد گردد. اما مقنن ایران برای برقراری نظم و امنیت و تأمین حقوق حاکمیت و شهروندان در فضای سایبر، حمایت کیفری را بر سایر حمایت‌های قانونی و عدم به کارگیری و توجه به ابزارهای غیرکیفری را مدنظر قرار داده است.(سعیدی، ۷۸:۱۳۹۶).

۳-الزامات و راهبردهای پیشگیرانه ایجابی و سلبی

افزایش قدرت تشخیص و تجزیه و تحلیل و نیز آشکار شدن نقش فناوری مدرن و توانایش در شناسایی هر چه سریعتر و دقیق تر فعالیت های متقلبانه و حملات سایبری، پیشرفت سیستم های امنیتی و فناوری مدرن که به توسعه ی امنیت و کارکرد سیستم های حفاظت الکترونیکی کمک می کند، آگاهی و آموزش، از آنجایی که فناوری روز نقش مهمی در افزایش آگاهی و آموزش کاربران در مورد خطرات جرایم سایبری ایفا می کند، از طریق روش های آگاهی الکترونیکی و منابع آموزشی، دانش و اطلاعات زیادی در مورد امنیت دیجیتال و اقدامات ایمن در اینترنت منتشر می شود.(بهرهمند و همکاران، ۱۴۹:۱۳۹۳). توسعه ی سیستم های تشخیص و پیشگیری با استفاده از تکنیک های یادگیری، ماشین یا هوش مصنوعی برای بهبود توانایی سیستم ها در تشخیص الگوهای غیرعادی و حملات سایبری و لزوم تبادل اطلاعات و همکاری و نیز تبادل اطلاعات بین طرف های ذینفع از جمله دولت ها، شرکت ها و موسسات دانشگاهی ست، زیرا همکاری آنها با هم می تواند به تقویت توانایی نظارت و مقابله بهتر با جرایم کمک کند.(آمری و همکاران، ۱۵۴:۱۳۹۹). تامین امنیت زیرساخت های فضای سایبری یک کشور یکی از پیش نیازهای امنیت پایدار آن کشور می باشد. ایجاد ساختارهای محلی، ارائه تدابیر امنیتی از مهمترین اقدامات برای پیشگیری از پدیده تروریسم سایبری قلمداد می شود. پدیده سایبر تروریسم از یک سو پدیده ای نوین و از سوی دیگر همان پدیده تروریسم به شمار می آید. تروریسمی که اقدامات خود را در فضای مجازی از سر می گیرد و با اهداف سیاسی و امنیتی در سطوح ملی و بین المللی و با نگاه فرافردی و جمعی دست به اقدامات مخرب می زند. (طریقی و طاهری، ۱۳۹۷: ۱۸)

در این زمینه اقدامات پیشـــگیرلنه نیز انجام می شـــود که عبارتند از: اقدامات محدودکننده یا ممانعت از دسترسی، اقدامات نظارتی برای شناسایی پرونده ها و پرونده های مشـکوک، اقدامات صـدور مجوز، ابزارهای ناشـناس سـازی و رمزگذاری، گشـت های اینترنتی و نظارت بر فضـای مجازی برای شـناسـایی موارد مشـکوک و پیشـگیری از جرایم احتمالی، آموزش عمومی، شـناسـایی و کنترل افراد. افزایش خطرات محســوس ارتکاب جرم، افزایش حمایت ها و مراقبت ها در فضـای مجازی و غیره. نقش اسـاسـی در پیشـگیری از جرایم سایبری دارند.

۵-۳ سازوکار اجرایی کیفرگذاری هدفمند

اهمیت راهبردی ســیاســت گذاری و تنظیم مقررات در حوزه کیفر گذاری هدفمند جایگاه ویژه ای در میان کشــورها دارد. با عنایت به لزوم ســیاســت گذاری کیفری جهت حمایت از انرژی می توان در ســه محور تولید، انتقال و توزیع انرژی این مباحث را مطرح گردد و انرژی به گونه های انرژی فســیلی نفت و گاز، انرژی برق، انرژی بادی و انرژی هسته ای مورد شناسایی و توجه قرار گیرد(موفق، ۱۴۰۰، ۱۷)

سیاست جنایی اجرایی در حوزه جرایم سایبری علیه انرژی این مهم را مدنظر قرار داده است که اختلاف نظرهای بسیار زیاد، فقدان اراده سیاسی دولت ها را برای ایجاد قواعد الزام آور مربوط به الزام رعایت حقوق بشــر برای اشــخاص حقوقی و مهار مقاومت بســیار زیاد آنان به ویژه اشــخاص حقوقی فراملی که نفوذ بسیار زیادی نیز بر قاعده گذاران ملی و بین المللی جرایم سایبری انرژی دارند در پی داشــته اســت. بهترین راه مقابله با اقدامات تروریســتی در محیط سایبری تقویت تدابیر امنیتی در شبکه های رایانه ای و اینترنتی، قوانین به روز حقوقی و تشکیل شورای مجازی یا سازمانی معتبر در ایران و عرصه بین المللی در مقابله با سایبری است. تروریسم و این امر مهم مستلزم انجام مطالعات در مورد تأثیر انقلاب اطلاعات بر امنیت ملی برای کاهش آســیب پذیری ها و تقویت امنیت ملی در برابر تروریسم سایبری است.(مجیدی، ۱۳۹۳: ۸۳)

۵-۴ فرایند تعیین میزان و نوع کیفر

با توجه به اهمیت محرمانه بودن داده های الکترونیکی و جرایمی که در پیرامون ما در عرصه جهانی در رابطه با آن رخ می دهد که امنیت و منافع کشورها را به طور عام و افراد به طور خاص تهدید می کند و خطر آن به سبب ارتکاب رایانه ای افزایش یافته اســت. انتقال از داده‌های کاغذی به داده‌های الکترونیکی مبتنی

بر یک راهبرد کیفری نوین برای رویارویی با وضـــعیت جدید در نتیجه رشـــد مستمر اینترنت است، زیرا حفاظت از این داده‌ها و دستیابی به امنیت بسترهای انرژی جدید اساس آن است. می توان گفت برای شناسایی جرایم علیه امنیت در فضای سایبر انرژی های نو سه راهکار وجود دارد، اول ارائه تعریف منطقی، دوم تعریف به مصـداق و سـوم برشـمردن ارزش‌های مورد حمایت.(دشـتی، ۱۴۰۰: ۵۴)

بر اساس این سه راهکار سیاست های کیفری مبتنی بر اصول کیفرگذاری و کیفردهی هستند و از طرفی یکی از سیاست‌های معروف کیفری سیاست کیفری عوام‌گرا اســـت و از آنجایی که عوام‌گرایی کیفری و قوانین مبتنی بر آن مبنی برجلب رضایت عمومی است احتمال نقض اصول کیفرگذاری و سزادهی در آن می‌رود، عوام‌گرایی کیفری در ایران با توالی فاسـد در پاسـخ‌دهی به جرائم علیه امنیت اعم از قانونگذاری‌های بدون پشـــتوانه علمی و تعیین مجازات سنگین و رسیدگی‌های شتاب‌زده به پرونده‌های کیفری و نقص در کار دستگاه عدالت کیفری همراه است. با توجه به تمایل دستگاه عدالت کیفری برای پاسخ سریع به جرائم، علی الخصوص جرائم علیه امنیت و راضی نگه‌داشتن افکار عمومی، عوام‌گرایی کیفری عامل مهمی در نقض حقوق متهم در جریان رسیدگی و اعمال مجازات سنگین علیه وی می‌باشد و همچنین استقلال قضات را هم خدشه‌دار می‌سازد.

با این توصیف در محیط سایبری و داده های محرمانه حوزه انرژی های نوپدید، با خلق دنیای مجازی موانع بسیاری از بین رفته و ارتکاب جرایم تسهیل شده است. فضای مجازی و دیجیتالی شرایطی را به وجود آورده که بزهکاران می توانند در مکان هایی غیر از جاهایی که آثار و نتایج اعمال آنها ظاهر می شـــود مرتکب جرم شـــده و به راحتی و با کمترین هزینه و اضـــطراب، بیشـــترین خسارات و صدمات رابه بار آورند و در عین حال ناشناخته باقی بمانند. آنچه در عوامل جرایم سایبری در انرژی های نو مورد تاکید است، شناسایی عوامل فردی و اجتماعی تاثیرگذار در این جرم اســت و در بحث پیشـگیری اجتماعی آنچه مدنظر است خنثی سازی انگیزه ارتکاب جرم در مرتکب می باشد و در پیشگیری وضعی، محیط ارتکاب جرم را مورد توجه قرار می دهد.(دوکوهکی، ۱۳۹۸: ۳۹)

یکی از آموزه‌های حقوق کیفری که در پرتو رویکردهای لیبرالیســـم و لیبرتاریانیســم پیرامون جرم انگاری و کیفرگذاری مرتکبین جرم مطرح شده بر

این اصـل اسـتوار اسـت که اسـاسـاً اسـتفاده از ظرفیت کیفر و مجازات باید به عنوان آخرین راهکار و نه واکنش بدوی و مقدماتی مورد اســتفاده قرار گیرد. اصـولاً اصـل آخرین راهکار تا چه میزان می‌تواند در تامین اهداف نظام عدالت کیفری از جمله اجرای عدالت یا پیشـگیری از جرم موثر باشـد. چنانچه اصـل آخرین راهکار درســت به‌کار گرفته شــود، می‌تواند به میزان موثری، منطبق با اهداف نظام عدالت کیفری، از جمله اجرای عدالت، پیشــگیری از وقوع یا تکرارجرم، اصــلاح مجرم و جبران بهتر زیان وارده به بزه‌دیده باشــد(تورانی و همکاران، ۶۵:۱۳۹۹).

بر اسـاس دو ضـابطه، محیط هدف جرایم سـایبری در حوزه انرژی و از طرفی آسیب های وارده را تقسیم بندی کنید. نقش مهم رایانه و اینترنت و خدماتی که این فناوری ها در اختیار بشــریت قرار می دهند باعث شــده اســت که بخش انرژی به این فناوری های جدید وابسته شود. به دنبال چنین وابستگی، خطراتی برای بخش انرژی ایجاد شـده اسـت که مهمترین آنها هدایت حملات سـایبری علیه این بخش است. بنابراین جهت جلوگیری و پیشگیری از حملات تبیین و صیانت از منابع انرژی در ایران باید نوعی ادغام در حوزه صلاحیت خط مشی گذاری دولتی و سیاست جنایی مشارکتی به وجود آید. البته به نظر می رسد که الزامات حقوقی، تقنینی، اجرایی، فنی، سـاختاری و محیطی در جرایم سـایبری در حوزه انرژی های نوپدید به ضرورت سنجی تدوین قوانین مجزای کیفری و کشف جرایم با ادله استناد پذیر دیجیتال در بستر حقوق انرژی های نو خواهد انجامید.(گودرزی و مقدادی، ۱۴۰۰:۴۵)

بنابراین جاسوسی و خیانت به کشور از رهگذر خرابکاری در تأسیسات فنی و زیر ســاختی انرژی های نو پدید از عناوین مجرمانه مهم علیه امنیت کشــورها می باشــد که به دلایل مختلف، جایگاه ویژه ای را در مقررات جزایی ایران و فرانسـه به خود اختصـاص داده اند؛ چرا که اسـتقلال و امنیت و تمامیت ارضـی کشـور و اسـاس حکومت را به خطر می اندازد و موجب فاش شـدن اسـرار و اطلاعات می شود (مجیدی، ۱۳۹۹: ۱۲).

نتیجه گیری

جرم انگاری عمل پسینی است که پیش از قانونگذاری الزاما مقنن از یک سری اصـــول و معیار مطابعت نمود و بی رویه به تحدید آزادی افراد نتازد امروزه در دنیای مدرن حفظ حقوق طرفین دعوی (بزه دیده، بزهکار) به همان لندازه مهم اســـت که حفظ حقوق جامعه و اعاده نظم ایجاب می نماید که قانونگذار در امور کیفری مداخله نماید مبانی نظری توجیه پذیر جرم انگاری و کیفرگذاری در پرتو اصـول متعددی اسـت که در لسـان حقوقدانان به اصـول محدودکننده آزادی نظیر: اصل ضرر، اصل حمایت قانونی، اصل مزاحمت عنوان شده است. در جرم انگـاری جرایم علیـه امنیـت در ایران قـانونگـذار بـا تخطی از نظریـات حاکم در برخی از جرم انگاری ها وجود ضـــرر را نادیده انگاشـــته و اقدام به اعمالی نظیر (اجتماع و تبانی) را حتی در مواردی که ضـرر به مجنی علیه نرسـد جرم انگاری نموده اسـت در کنار اصـول کیفرگذاری در جرایم علیه امنیت باید معیارهای جرم انگاری در این حوزه نیز مورد واکاوی قرار داد معیارهای جرم انگاری در هرکشـور و جامعه بسـته به نوع و قالب حکومت متفاوت از هم می باشـد. اگرچه وجود قوانین کیفری برای شـناخت هنجارها و رفتارهای جامعه ضـروری اسـت؛ اما برای ایجاد جامعه ای قانونمند نمی توان تنها از مکانیسـم جرم انگاری چندگانه استفاده کرد. زیرا هر قانون جزایی، صـرف نظر از ترتیب فســـاد خود، آزادی افراد را محدود و از بین می برد و حوزه اختیار و کنترل حکومت را گســـترش می دهد. جرم انگاری بیش از حد در کشـــور ما باعث بحران تورمی قوانین کیفری شـده اسـت. بحران فوق، انجام وظیفه اسـاسـی نظام عدالت کیفری یعنی تضـــمین حقوق شـــهروندان و اجرای عدالت کیفری را با مشـــکل مواجه کرده اســـت.اما تدوین قوانین در حوزه انرژی های نو توســـط مراجع غیر ذی صلاح از جمله دیوان عالی کشور در مقام وحدت رویه، مجمع تشخیص فرصت، شورای عالی انقلاب فرهنگی و سایر مراجع به این انباشت کیفری دامن می زند. از سوی دیگر موضوع تورم کیفری به عنوان چالشی برای نظام حقوقی ایران، عوامل ایجاد کننده این پدیده و آثار آن و نیز برنامه ریزی جنایی راه های خروج از بحران مذکور در ســایه جرم شــناســی کیفری مدرن است.

ســیاســت گذاری تقنینی ایران در حوزه انرژی با تکیه بر به روزترین اطلاعات ممکن و توجه به جرایم سایبری در این حوزه مورد تحلیل قرار گیرد و با توجه به تجارب کشـــورهای موفق و نهادهای مرتبط با حوزه انرژی های تجدیدپذیر راهکارهایی با توجه به شـــرایط انرژی خاص ایران و نیازهای این کشـــور ارائه شود. سیاست گذاری کیفری جهت حمایت از انرژی در سه محور تولید، انتقال و توزیع انرژی از یک سو و تنظیم سیاست های کیفری و حوزه قانونگذاری در

جرایم سایبری حوزه انرژی از ارکان جهت ساز به شمار می آید. الزامات سیاست جنایی در مقابله با جرایم سایبری در حوزه انرژی از طریق کیفرگذاری کارآمد، بهره گیری از قضات با تجربه، نظام پیشگیری موثر و هم افزایی با پلیس فناورانه در حوزه جرایم سایبری انرژی می باشد.

بارزترین یافته پژوهش حاضر عدم ثبات در یک مفهوم واحد از جرایم سایبری بود که شاید دلیل این امر احتمال بروز جرایم جدید مرتبط با دنیای مجازی و قرارگرفتن در محدوده این جنایات، فقدان جرائمی مانند جرم تروریسم به عنوان یک جرم مستقل در حقوق کیفری ایران مشاهده می شود و همچنین جرمی تحت عنوان خیانت به کشور در قانون مجازات اسلامی جرم انگاری نشده است. لیکن در حقوق ایران و حتی پیش نویس لایحه تعزیرات ۱۴۰۱ شاهد مصداقی از جرایم سایبری به عنوان یک بزه مستقل نیستیم.

در مجموع می توان گفت که بارزترین آنها عدم ثبات در مفهوم واحد جرایم سایبری بود که شاید دلیل احتمال وقوع جرایم جدید مرتبط با دنیای مجازی و قرار گرفتن در محدوده این جرایم باشد. پیشنهاد تصویب قانونی به طور خاص برای جرایم سایبری در حوزه انرژی های نوظهور به منظور تنظیم جرایم الکترونیکی در تمام جنبه های ماهوی و رویه ای آن است، زیرا جرایم سایبری خود به تنهایی جرم خاصی هستند.

منابع

– آقابابایی، حسین، ۱۳۸۹، قلمرو امنیت در حقوق کیفری، تهران: پژوهشگاه فرهنگ و اندیشه اسلامی.

– ارشدی، علی یار، بقایی، بهزاد و همکاران، ۱۴۰۰، قوانین برق (تمامی قوانین در یک قانون جامع)، تهران: پژوهشگاه نیرو.

– اسکندری، حسین، ۱۳۹۰، راهکارهای دفاع سایبری و قانون جرائم رایانه‌ای، تهران: بوستان.

– السان مصطفی، ۱۳۹۸، حقوق فضای مجازی، تهران: موسسه مطالعه و پژوهش های حقوقی شهر دانش.

– الهوردی، فرهاد، ۱۳۹۶، حقوق کیفری سایبری، تهران: جنگل.

– امینی زارع، رامین، ۱۳۹۲، هوای پاک با انرژی پاک، نشریه اطلاعات سیاسی– اقتصادی.

– بابک پورقهرمانی، الناز، ۱۳۹۸، سیاست های نمادین معاهدهٔ جرایم سایبری شورای اروپا، فصلنامهٔ مطالعات بین المللی، ش۲.

– بوگانسکی، میتکو، پترسکی، دریژ، ۱۳۹۴، تروریسم سایبری، تهدید علیه امنیت جهانی، ترجمهٔ ندا نیازمند، مجموعهٔ مقالات تروریسم‌شناسی (رویکرد حقوقی– فلسفی)، تهران: نگاه بیّنه.

– پاکزاد، بتول، ۱۳۹۰، تروریسم سایبری تهدیدی نوین علیه امنیت ملی، تهران: گسترش تولید علم.

– تبریزی، صادق، عالی‌پور، حسن، طهماسبی، جواد، فضلی، مهدی، الهی منش، محمدرضا، ۱۴۰۱، اصل قانون‌مندی توقیف داده و سامانه در فرایند کیفری، جلوه‌ها و تضمین‌ها، مجله تعالی حقوق، ش ۲.

– تورانی، بیتا، عطاشنه، منصور و مرادی، مریم، ۱۳۹۹، بررسی چالش های توسعه اقتصادی و اصلاحات قانونی استفاده از انرژی های تجدیدپذیر، تهران: نشریه جامعه شناسی سیاسی ایران.

– جعفری، افشین، ۱۳۹۷، تحدید حملات سایبری، تهران: مجد.

– حاجی‌رضائی، علی، ۱۴۰۰، جایگاه تروریسم سایبری با نگاهی به اسناد بین‌المللی، تهران: قانون‌یار.

– حبیب‌زاده، محمدجعفر، ۱۴۰۰، حقوق جزای اختصاصی جرائم علیه اموال و مالکیت، تهران: سمت.

– دبیرنیا، علیرضا، ۱۳۹۸، جایگاه قوانین برنامه توسعه در قانون اساسی ایران، برنامه ریزی در راستای وظایف قوه قضاییه، مجله حقوقی دادگستری.

– دوکوهکی، محمدرضا، ۱۳۹۸، بررسی جزایی جرائم رایانه‌ای و سایبری، تهران: قانون یار.

- زارع، مهدیه، ۱۳۹۴، نقش انرژی های تجدیدپذیر در حفاظت از محیط زیست ایران، پایان نامه کارشناسی ارشد، دانشگاه شهید بهشتی.
- سلطانی، لادن، ۱۳۹۳، جرائم علیه صحت و تمامیت داده‌های رایانه‌ای در فضای سایبر در نظام حقوقی ایران و اسناد بین‌الملل، پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی اصفهان.
- شریفی خضارتی، امیر، ۱۳۹۸، تروریسم (رویکرد سیاست تقنینی)، تهران: اندیشه عصر.
- طریقی، نوشین، طاهری، ابوالقاسم، ۱۳۹۷، دیپلماسی انرژی در اسناد راهبردی سیاست خارجی ایران، تهران: سیاست جهانی.
- قرشی، سیدعلی، شبرو، مریم، ۱۳۹۳، مقدمه ای بر نحوه بکارگیری فن آوری اینترنت اشیاء در شبکه هوشمند صنعت برق کشور، بیست و نهمین کنفرانس بین‌المللی برق، تهران.
- گودرزی بروجردی، محمدرضا، مقدادی، لیال، ۱۴۰۰، درآمدی بر قانون مجازات فرانسه،تهران: انتشارات خرسندی.
- مجیدی، سیدمحمود، ۱۳۹۹، حقوق کیفری اختصاصی تطبیقی جرایم علیه امنیت، تهران: میزان.
- مجیدی، سیدمحمود، ۱۳۹۳، جرایم علیه امنیت. تهران: میزان.
- محبی، جلیل، ریاضت، زینب، ۱۳۹۵، مبانی و مدل کیفرگذاری تعزیری مطالعه موردی در جرایم علیه امنیت، فصلنامه آفاق امنیت، دوره ۹، ش ۳۳.
- محقق داماد، سیدمصطفی، ۱۴۰۰، قواعد فقه، تهران: اسلامیه.
- هریسن داینیس، هیثر، ۱۳۹۵، جنگ سایبری و حقوق جنگ، ترجمهٔ سعید حکیمی‌ها و هومان شاهرخ، تهران: میزان.
- هلیلی، خداداد، ۱۴۰۰، فناوری‌های نوظهور سایبری و تهدیدات ناشی از بکارگیری آنها در سازمان‌های دفاعی- نظامی، فصلنامه علمی مطالعات جنگ. دوره ۳، ش ۱۱.

- S.C.E. Jupe; A. Michiorri; P.C. Taylor (2017). "Increasing the energy yield of generation from new and renewable energy sources". Renewable Energy. 14 (2): 37–62.
- Zehner, Ozzie (2012). Green Illusions. Lincoln and London: University of Nebraska Press. pp. 1–169, 331–4.
- Wasielewski, Michael R., Styring, Stenbjorn (2019).",Energy and environment policy case for a global project on artificial photosynthesis",. Energy &, Environmental Science. RSC Publishing.

Sütterlin, B., Siegrist, Michael (2017). ",Public acceptance of renewable energy technologies from an abstract versus concrete perspective and the positive.