

فصلنامه مطالعات سیاسی
سال سیزدهم، شماره ۵۲، تابستان ۱۴۰۰
صفحات: ۸۱-۱۰۰
تاریخ دریافت: ۱۴۰۰/۱/۱۰؛ تاریخ پذیرش نهایی: ۱۴۰۰/۳/۲۹
مقاله: پژوهشی

تحقق امنیت انسانی از رهگذر امنیت در اقتصاد سیاسی بین الملل

هادی مسعودی فر* / علیرضا آرشی پور** / مسعود راعی دهقی***

چکیده

با توجه به تحولات روابط بین المللی در جهان مدرن و به ویژه، با توسعه نیازهای متقابل جامعه بشری در زمینه های اجتماعی، اقتصادی، سیاسی، فرهنگی و همچنین توسعه مفهوم امنیت ملی از رویکردی صرفاً نظامی به رویکرد زیست محیطی و اقتصادی، و با توجه به ورود جوامع بشری به عرصه رقابت های تجاری و فن آورانه، به نظر می رسد که لازم است طبقه بندی جدیدی از مفهوم امنیت انسانی که با واقعیات موجود در توسعه تجارت و اقتصاد سیاسی بین الملل سازگار تر است، ارائه شود. بر همین اساس لازم است ابتدا گذر از مفهوم امنیت ملی به سمت مفهوم امنیت اقتصادی را مورد بررسی قرارداد و سپس مفاهیم نوین در حوزه امنیت انسانی را پیشنهاد و تشریح نمود. بر همین اساس در این تحقیق، مفهوم امنیت انسانی از ضروریات صرفاً نظامی و زیست محیطی عبور کرده و با رویکردی نوین در قالب مفهوم امنیت تجاری با هدف محافظت از داده های تجاری مطرح می گردد. همچنین در این نوشتار که مبتنی بر روش استقرایی و مطالعات کتابخانه ای تدوین شده است، اصل پیشگری به عنوان روشی نوین جهت جلوگیری از درز داده های اطلاعات تجاری و مالکیت معنوی با هدف تحقق امنیت تجاری مطرح شده است.

کلیدواژه‌ها: امنیت انسانی؛ امنیت اقتصادی؛ امنیت ملی؛ روابط بین الملل؛ مالکیت معنوی.

* گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران.

** گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران (نویسنده مسؤول).

a.arashpour@ase.ui.ac.ir

*** گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران.

۱. بیان مسأله

تردیدی نیست که امروزه کشورهای جهان به شکل قابل توجهی از جهت اقتصادی به یکدیگر وابسته شده اند که این خود تحقق مفهوم جهان کشوری را به همراه داشته به نحوی که در این چرخه، کشورهای توسعه یافته به مواد اولیه، نیروی کار ارزان و نیز بازارهای در حال شکل گیری کشورهای کم تر توسعه یافته نیازمند هستند و در مقابل کشورهای در حال توسعه نیز به محصولات صنعتی، دانش و تکنولوژی کشورهای پیشرفته نیازمندند که این خود اهمیت زنجیره ای از منافع مشترک، زیست اجتماعی و پایداری در امنیت جهانی را اثبات می کند که در این اکوسیستم فعال، امنیت تجارت بین الملل از مهم ترین ضروریات به حساب می آید. در بحث این ارتباط، این مسأله تاکنون کم تر مورد توجه قرار گرفته است که اگر مفهوم امنیت انسانی را تنها در مواجهه با مخاطرات حاصل از فعالیت های نظامی، بستر های زیست محیطی و طبیعی در نظر بگیریم، یک جامعه مدرن که در تعامل با پیوندهای تجاری و اقتصادی جهان قرار دارد، در برخورد با خطر درز اطلاعات تجاری که خود از عدم محافظت دقیق اسرار تجاری حاصل می شود، چه رویکردی را باید مد نظر قرار دهد تا میزان آسیب پذیری چرخه اقتصادی و در امتداد آن زیست اجتماعی آن جامعه کاهش پیدا نماید. یکی از دلایل عدم توجه به آسیب های حاصل از عدم محافظت دقیق بر داده های تجاری، تأکید و تمرکز ویژه بر بعد زیست محیطی و نظامی مفهوم امنیت انسانی است که این خود می تواند در نتیجه بی توجهی به روند توسعه مترقیانه در مطالعات پیرامون امنیت انسانی و حقوق بین الملل و همچنین تمرکز بر بعد نظامی در مقوله امنیت ملی^۱، حاصل آید. بررسی میزان اثرپذیری حوزه امنیت ملی کشورها از موضوعات پیرامون حفاظت از امنیت داده های اطلاعات تجاری می تواند از جمله نگرش های نوین در برخورد با مولفه های برهم زننده ثبات اقتصادی در جوامع مدرن باشد زیرا درز اطلاعات تجاری بنگاه های اقتصادی، مراکز توسعه فن آوری اطلاعات و چرخه تولید کالا و خدمات می تواند پیشرفت اقتصادی و به تبع آن، امنیت زیست اجتماعی یک جامعه را به شدت تحت خطر قرار بدهد. بر همین مبنا لازم است، تحقق امنیت انسانی را مبتنی بر رویکرد تازه ای که در آن بتوان امنیت پایدار اقتصادی و تجاری برای نسل های آینده را تضمین کرد، تدوین نمود. از همین رو جنبه نو اورانه تحقیق حاضر این است که معیار ها و اصول مورد احترام در حوزه مطالعات تجارت و اقتصاد بین الملل با رویکرد محافظت از امنیت داده های اطلاعات

1. National Security

تجاری با هدف تضمین تحقق الگوهای امنیت انسانی همراه است که در آن از یک سو اهمیت نقش محافظت با تأکید بر اصل پیشگیری از درز داده های تجاری و نیز کاهش آسیب پذیری اقتصاد جامعه از طریق اجبار در رعایت مبانی مالکیت فکری مورد تأکید قرار می گیرد.

برای آغاز بحث لازم است که ابتدا برداشتمان از مفهوم امنیت اقتصادی¹ و امنیت تجاری روشن شود. سپس با توجه به تعریف امنیت انسانی و رابطه امنیت اقتصادی با تحقق مفهوم امنیت تجاری این پرسش مطرح می گردد که مسائل و وقایع پیرامون موضوعات زیست اقتصادی و تجارت قابل اطمینان چه نقشی در تحقق مفهوم امنیت اجتماعی و انسانی دارند؟ رعایت اصل پیشگیری در محافظت از داده های اطلاعات تجاری چه تاثیری در تحقق امنیت تجاری دارد؟ و آیا می توان فرایند تحقق امنیت تجاری را مبتنی بر محافظت از داده های اطلاعاتی به صورت نهادی مستقل اجرا کرد یا بایستی این مکانیزم را مبتنی بر مفهوم امنیت ملی، وظیفه ای بر عهده دولت دانست؟ آنچه که در رهگذر پرسش های مطروحه قابل توجه است، رسیدن به نگرشی تازه در برخورد با محافظت از داده های اطلاعاتی مبتنی بر مبانی مالکیت فکری در برخورد با حملات سایبری است که این خود نیازمند نگرشی و نو در این زمینه است.

در مقدمه می توان گفت که مفهوم امنیت تجاری و مفهوم اصل پیشگیری در حقوق بین الملل اقتصادی دارای استاندارد هایی هستند که با پردازش هریک به طور دقیق می توان به تأثیر تحقق امنیت تجاری در تضمین تحقق مفهوم امنیت انسانی دست یافت. در این بین نباید این نکته را از نظر دور داشت که مفهوم اقتصاد بازار آزاد مبتنی بر رقابت بین مراکز تحقیقات و توسعه و نیز سرعت در دستیابی به تکنولوژی روز استوار است که این خود یک امر مورد تایید و مشروع حقوقی است زیرا هیچ شخصیت حقوقی تجاری پیشرفت و توسعه رقبا خود را بر نمی تابد اما میزان مشروعیت این رقابت بایستی به لحاظ حقوقی مورد ارزیابی قرار بگیرد. انعکاس اصل پیشگیری به عنوان یک اصل مترقیانه در حوزه مطالعات حقوق بین الملل اقتصادی با مقوله امنیت تجاری در راستای تحقق امنیت انسانی از نوآوری های دیگر این تحقیق به شمار می رود که منجر به معرفی رویکردی تازه در برخورد با مخاطرات غیر نظامی در برهم خوردن امنیت ملی توسط جوامع بشری است.

در این تحقیق که مبتنی بر بررسی اسناد و مدارک علمی همراه با رویکرد زمینه ای استوار است، تلاش شده است روش بکار رفته در مسیر تحلیل مباحث با تکیه بر موضوعات نظری جهت دست یافتن به رویکردهای نوین و آینده نگرانه همراه باشد. تأکید بر تحلیل های نوآورانه در مباحث حقوق بین الملل اقتصادی می تواند مبتنی بر استدلال استقرایی^۱، زمینه برای توسعه تدریجی در مطالعات آینده را نیز فراهم آورد.

۲. مفهوم شناسی امنیت اقتصادی

امنیت اقتصادی یکی از مهم ترین ابعاد امنیت ملی و از اصول مهم و زیرساخت های اساسی کشورها برای دستیابی به توسعه اقتصادی و ارتقای سطح رفاه اجتماعی محسوب می شود و از این رو همیشه مورد توجه سیاست گذاران و برنامه ریزان اقتصادی کشورها بوده است (Ezati & Dehghan, 2008: 93). با توسعه روابط فرهنگی، اقتصادی و اجتماعی میان جوامع، شاهد شکل گیری بستری بین المللی از مشارکت در امور حیاطی زندگی بشر هستیم که می توان از آن با عنوان جامعه مدنی بین المللی^۲ یاد کرد. این جامعه در هم تنیده مبتنی بر نیازهای مشترک و همزیستی ساختاری بنا گردیده است. امروزه تقریباً هیچ کشوری را نمی توان یافت که تمام یا بخشی از نیازهای خود را به طور فردی و انحصاری تامین نماید. بنابراین در همین نقطه است که وابستگی متقابل کشورها در امور اقتصادی به یکدیگر، در اشکال گوناگونی نمایان می گردد که اهم آن ها عبارت اند از: تجارت کالا، خدمات، سرمایه گذاری مشترک و بهره مندی از نیروی علمی و نیروی انسانی. افزایش روزافزون نیاز مشترک جامعه بشری به اقتصاد مشترک از عوامل متعددی نشاط می گیرد که از آن جمله می توان به توسعه تکنولوژی و فن آوری اشاره کرد که این خود مقدمه ای برای توسعه روابط اقتصادی می شود زیرا کشورهای کم تر توسعه یافته یا حتی کشورهای توسعه یافته به تبادل و انتقال تکنولوژی نیازمندند. تحقق جامعه مشترک مدنی در عرصه بین الملل نیازمند تحقق جهانی شدن بازار، حقوق و شرکت های چند ملیتی^۳ است. البته نباید فراموش کرد که این سه در رابطه عرضی از هم قرار دارند. یعنی هیچیک از آن ها اعتبار خود را از دیگری به دست نمی آورد. به طور مثال امروزه شرکت های چند ملیتی فراوانی در سطح جهانی به فعالیت های اقتصادی مشغول اند بدون آنکه مقررات واحدی در

1. Inductive Reasoning
2. International Civil Society
3. Mmultinational Companies

خصوص نحوه فعالیت آن ها وجود داشته باشد (Braithwaite, et al, 2000: 85). همین امر ضرورت تحقق امنیت اقتصادی را نمایان می سازد. در صورت فقدان امنیت اقتصادی، امکان سوء استفاده از تضادها و تعارضات قانونی فراملی در عرصه تجارت بین الملل بالا رفته و این خود بی ثباتی اقتصادی را رقم می زند. در سایه عدم بی ثباتی اقتصادی، پدیدارهای اجتماعی و سیاسی نیز می تواند تحت تأثیر قرار گرفته و جنبه عدم مشروعیت تعامل اقتصادی بین جوامع با ضریب پایین امنیت اقتصادی را فراهم آورد. از طرفی دیگر: فعالان اقتصادی به مفاهیمی از قبیل خروج سرمایه از کشور و نیز فرار مغزها می اندیشند و هر فعال اقتصادی سعی خواهد کرد که سرمایه و کار خود را به مکان های امن تر منتقل نموده و با تبدیل دارایی های خود به پول نقد و دارایی خارجی، هرگونه اثرات منفی حاصل از نا امنی را به حداقل برساند (Jelodar, 2014). از همین رو تحقق امنیت اقتصادی می تواند در بروز عناصر برهم زننده مفهوم امنیت ملی نیز تأثیرگذار باشد زیرا: امنیت ملی بیانگر توانایی نهادهای سیاسی، حقوقی و اقتصادی مربوطه در حفاظت از منافع اشخاص کلیدی در سنت ها و ارزش های اقتصاد ملی است. بنابراین، توسعه آن باید در بستر کلی تشکیل دولت مبتنی بر امنیت ملی دیده شود (Litvinenko, 2013: 9-15). براین اساس، امنیت اقتصادی زیرمجموعه ای از مفهوم امنیت ملی است و از آنجا که تضمین امنیت ملی بر عهده دولت است، بایستی مبتنی بر همکاری با پارامترهای موجود در امنیت اقتصادی صورت پذیرد. اما معمولاً از نظر دولت ها، امنیت اقتصادی مطلق، اساساً وجود نداشته زیرا تهدیدات پیرامون امنیت اقتصادی، هم از خارج و هم از درون حاکمیت ملی، قابل بروز و رخداد است و این می تواند پایداری در تحقق امنیت اقتصادی را به طور جدی تحت تأثیر قرار دهد. اما مبتنی بر رویکردی جامع، عوامل اصلی امنیت اقتصادی در هر کشور عبارتند از: موقعیت جغرافیایی آن، منابع طبیعی، پتانسیل های صنعتی و کشاورزی، میزان توسعه اجتماعی و جمعیت شناسی، کیفیت مدیریت عمومی و تحقق توسعه علمی و فن آوری. بر همین اساس می توان گفت: کشورهای همچون روسیه، ایالات متحده، ژاپن، چین و نیز کشورهای اتحادیه اروپا موقعیتی پیشرو در جهان از نظر پتانسیل صنعتی، حجم تولید محصولات کشاورزی و منابع طبیعی دارند همچنین آن ها از موقعیت جغرافیایی بی نظیری برخوردار هستند که به امنیت اقتصادی آن ها کمک می کند (Grigoreva & Fesina, 2013: 940-948). از طرف دیگر تجزیه و تحلیل روندهای توسعه روابط اقتصادی جهان، پیشرفت علمی و فناوری در اقتصاد، تعامل در فرایند ادغام جهانی و

تأثیر این فرآیندها بر اساس رویکرد امنیت ملی جامعه ی جهانی، به برجسته کردن عوامل اصلی امنیت اقتصادی منجر گردیده است (Reshetova & Krutik, 2011: 112). اما آنچه که باید در نظر داشت این نکته است که فرایند تحقق امنیت اقتصادی به عملکرد دولت ها در گذشته، سیاست های اجرایی کنونی و برنامه های توسعه برای آینده مرتبط است. آنچه که در این میان بسیار حائز اهمیت است، سیاست های محافظتی است که دولت ها برای عدم درز اطلاعات مربوط به توسعه فن اوری بکار گرفته که می توان از آن با عنوان سیاست های تحقق امنیت تجاری نام برد.

۳. مفهوم شناسی امنیت تجاری^۱

تحقق مفهوم امنیت اقتصادی، وابستگی دارد به تحقق امنیت در تجارت کالا و خدمات. یکی از مهم ترین اجزاء اقتصاد مولد در هر جامعه ای، فعالیت های تجاری و بازرگانی است که خود به بخش های «تحقیق و توسعه»، «تولید»، «صادرات»، «واردات» و «انتقال تکنولوژی» تقسیم می گردد. تحقق امنیت در هریک از حوزه های نام برده، ضرورتی اجتناب ناپذیر است که خود مقدمه ای در تحقق ثبات و امنیت در دیگری است. به طور مثال: تحقق امنیت در فرایند تحقیق و توسعه هر واحد تولیدی و تجاری مقدمه ای بر تحقق امنیت در فرایند تولید و نیز امنیت در فرایند صادرات است. لذا می توان گفت که مبتنی بر شاخصه امنیت، رابطه بین اجزاء مرتبط با فعالیت تجاری یک رابطه طولی است به نحویکه عملکرد مطلوب هریک از اجزاء، وابسته به تحقق امنیت در واحد قبل از خود است.

کلیدی ترین رکن امنیت در فرایند فعالیت های تجاری و بازرگانی، محافظت از داده های اطلاعاتی و جلوگیری از نقض مالکیت معنوی^۲ و درز اطلاعات محرمانه است. اگرچه همه شرکت ها با خطر از دست دادن مالکیت معنوی و اطلاعات محرمانه در مورد تجارت روبرو هستند، اما برخی از بخش ها مانند امور مالی، مواد ترکیبی و شیمیایی، هوا فضا، انرژی، دفاع و فناوری اطلاعات، به احتمال زیاد مورد هدف قرار می گیرند و اطلاعات طبقه بندی شده خود را از دست می دهند. ضرر و زیان حاصل از درز اطلاعات به مراتب از درآمدزایی حاصل از تجارت نا ایمن، بیشتر است، بدین شکل که با استفاده از مواد اولیه شیمیایی، می توان فرمول های اختصاصی

1. Commercial Security

2. Intellectual Property

را به راحتی کپی کرده و یا دارای اطلاعات حساس در مورد تجارت شد (Chiara, 2017: 129-132). اما قرار گرفتن مفهوم امنیت تجاری در طبقه بندی های مرسوم مانند مفهوم امنیت ملی، امری مهم است که می تواند تحقق آن را تحت تأثیر خود قرار بدهد. از آنجا که حاشیه میان اسرار تجاری و اسرار دولتی در میان نظام های سیاسی مبتنی بر دموکراسی ها و کشورهای اقتدارگرا همواره مبهم است، در این میان سرقت های مخفی تجاری به طور فزاینده ای در نیمه راه بین امنیت ملی و جاسوسی بازرگانی طبقه بندی می گردند (Peter k, 2015: 133-134). در راستای مکانیزه نمودن فرایند حفاظت از داده های اطلاعات تجاری دو رویکرد مهم وجود دارد:

رویکرد اول: این رویکرد معتقد است که مفهوم امنیت تجاری بایستی ذیل مفهوم امنیت ملی قرار داده شود تا بین منافع ملی و منافع تجاری رابطه مستقیم برقرار شده به نحویکه دولت ها متولی اصلی در راستای حفظ اطلاعات تجاری و تحقق امنیت اقتصادی معرفی گردند. این رویکرد را می توان در الگوی محافظت از داده های تجاری در کشور چین مشاهده نمود: آنجا که محافظت از اطلاعات تجاری برای مدت زمانی طولانی با اسرار دولتی، همپوشانی دارد (Ping Xiong, 2016: 252-262).

رویکرد دوم: این رویکرد برعکس رویکرد اول، معتقد است که فرایند امنیت تجاری بایستی مستقل از نهاد امنیت ملی طبقه بندی شده و در نتیجه بایستی ابتکار عمل در محافظت از اطلاعات تجاری مبتنی بر مبانی مالکیت فکری به بخش غیر دولتی سپرده شده به نحویکه هریک از بنگاه های تجاری به طور دقیق برابند محافظت و ممانعت از درز اطلاعات تجاریشان را خود بر عهده بگیرند. در راستای این رویکرد می توان به الگوی پیاده شده در ایالات متحده آمریکا اشاره نمود که شرکت های تجاری در فرایند تحقیق و توسعه و همچنین تولید و صادرات موظف اند که اسرار تجاری خود را حفظ کرده و دولت نیز در راستای درز اطلاعات این شرکت ها هیچ مسؤولیتی بر عهده ندارد.

شناخت دو رویکرد فوق قابل تأمل است اما آنچه که از اهمیت بالاتری برخوردار است، رویکرد قانونی به محافظت از داده های اطلاعاتی و نیز حفظ امنیت تجاری در اقتصاد است. تفکیک بین دو رویکرد ذکر شده در بالا می تواند به شناخت مختصات مفهوم امنیت تجاری به ما کمک کند اما در عمل نگرش قانون به امنیت تجاری است که اهمیت دارد. بر همین مبنا، چنانچه هرکس محصول تجاری را که قبلا به ثبت رسیده است را تولید کند، صرف نظر از اینکه آگاهی آن ها

در باره ثبت اختراع به اندازه کافی بوده است یا نه، قطعاً نقض حق ثبت اختراع است اما مبتنی بر رویکرد قانونی، محاکمه تنها در صورت سرقت و تکثیر آن صورت می پذیرد (Herbert J, 2015: 102). آنچه که در این میان باید در نظر گرفت این است که حتی اگر مفهوم امنیت تجاری را ذیل مفاهیم حاکمیتی مانند امنیت ملی و منافع ملی قرار ندهیم بازهم نقش دولت ها در بعد پیشگیرانه، از بین نرفته و حذف نمی گردد، برعکس امروزه رویکرد رایج در استراتژی پنهان تجارت ملی این است که دولت می بایستی پشتیبانی نرم داشته باشد. بر همین اساس است که در برخی از طرح های امنیت سایبری، شرکت ها بایستی طبق قانون (مقررات سخت) استانداردهای از پیش تعیین شده مربوط به فضای مجازی را رعایت کرده و همچنین این شرکت ها موظف اند که بندهای مربوط به امنیت سایبری هنگام صدور مجوز های دولتی، به امضا برسانند. در همین راستا می توان به دستور العمل های کمیسیون تجارت فدرال در ایالات متحده آمریکا اشاره کرد که مقرر کرده شرکت های ناسازگار با استانداردهای حفاظت داده باید مبتنی بر الگوی ایالات متحده جریمه شوند. بر همین مبنا کمیسیون تجارت فدرال، اقدامات حقوقی را بر علیه شرکت هایی اعمال می کند که در فرایند تولید و فروش محصولات، ویژه گی های مربوط به رعایت امنیت داده را به طور کافی رعایت ننموده اند (Determann, 2017: 143). بنابراین می توان اینگونه در نظر گرفت که امنیت تجاری در مختصاتی بین مفهوم امنیت ملی و ضرورت های پیشگیرانه در بخش خصوصی متجلی می گردد و نمی توان تنها آن را مولد رویکرد های ملی یا خصوصی دانست. از این رو مفهوم امنیت تجاری تأثیر مستقیمی بر تحقق مفهوم امنیت انسانی دارد زیرا انعکاس عملکردهای پیشگیرانه در ممانعت از درز اطلاعات تجاری می تواند در کوتاه مدت تأثیر مستقیمی بر رونق تجارت ایمن و در نتیجه شاخصه امنیت اقتصادی داشته باشد. بر همین مبنا می توان با رویکردی تازه مفهوم امنیت انسانی را مورد تحلیل قرار داد. رویکردی که در آن بعد امنیت تجاری از غلظت بالاتری برخوردار است. با این مقدمه می توان در ادامه مفهوم امنیت انسانی را مورد بررسی قرار داد.

۴. مفهوم شناسی امنیت انسانی مبتنی بر رویکرد امنیت تجاری

برای درک بهتر مفهوم امنیت انسانی، می توان این مفهوم را در کنار مفهوم توسعه انسانی مورد ارزیابی قرار داد. مبتنی بر رویکرد فهرست توسعه انسانی سازمان ملل متحد موسوم به

(HDI)¹: توسعه انسانی مبتنی بر استاندارد مناسب برای زندگی سالم، طولانی و مبتنی بر دانش ارزیابی شده است (UN. Human Development Reports, 2011: 130).

بر همین مبنا توسعه انسانی مفهومی به مراتب گسترده و اساسی تر از شاخصه هایی همچون درآمد ملی یا تولید ناخالص داخلی، به حساب می آید. مفهوم توسعه انسانی بر ایجاد بستری ایمن برای شکوفایی استعدادهای انسان تأکید داشته و رویکرد جامعه بین المللی و سازمان ملل متحد بر آن است که اساساً انسان سرمایه اصلی جامعه بین المللی است و بایستی در راستای توسعه و پایداری در تحول مترقیانه آن، همکاری و وفاق بین المللی حاصل گردد. حال در این میان شاخصه امید به زندگی به عنوان یک عنصر اساسی در تحقق مفهوم توسعه انسانی مد نظر قرار گرفته است. با این رویکرد افزایش طول عمر آدمی از ضروریات جامعه بشری است. بنابراین تحقق امنیت زیستی و کاهش ریسک آسیب های بالقوه به پیکره حیات آدمی از مهم ترین اهداف جامعه بین المللی به حساب می آید. آنچه که در این مقیاس حائز اهمیت است، تحقق دانش انسان پیرامون مفهوم امنیت انسانی است. البته مفهوم امنیت انسانی بسیار متغیر است و این خود برداشت های بعضاً متضادی از آن را پدید می آورد. اما بنظر می توان مفهوم امنیت انسانی را مبتنی بر درک از مفهوم توسعه انسانی مورد شناخت دقیق تر قرار داد. آنچه که در تحقق مفهوم توسعه انسانی حائز اهمیت است، اشتراک در توسعه اقتصادی بین تمام آحاد مردم یک جامعه است. که خود می تواند توسعه سلامت و بهداشت را رقم بزند. به گفته راوی کانبور، نبردهای سیاسی در بانک جهانی در زمینه توسعه و کاهش فقر منجر به توافقی کلی شده است که آموزش و بهداشت و سلامت به اندازه ثروت در ارزیابی نتیجه توسعه مهم هستند (Kanbur, 194-1083 : 2001).

اما آنچه که می تواند به عنوان حلقه اتصال بین آموزش، بهداشت و سلامت در این چرخه نقش آفرینی نماید، تحقق تجارت پایدار است که خود از طریق تحقق مفهوم امنیت تجاری حاصل می گردد. بنابراین حلقه اتصال بین مفهوم امنیت انسانی مبتنی بر رویکرد امنیت تجاری، تحقق مفهوم توسعه انسانی است که این دو را به یک دیگر مرتبط می سازد. آنچه که در این مسیر می تواند به عنوان مانع بر سر راه تحقق امنیت تجاری در نظر گرفته شود، برهم خوردن شاخصه های مرتبط با مفهوم امنیت انسانی است. باید این نکته را مورد تأکید قرار داد که امنیت انسانی یک وضعیت نسبی است در حالیکه توسعه یک فرایند است. بنابراین امنیت بشر

1. The Human Development Index (HDI)

تحت تأثیر فرآیندهای توسعه است. موانع موجود بر سر راه توسعه، ناامنی های انسانی را ایجاد می کند و بنابراین پایداری در پیشرفت بشر باعث تقویت مفهوم امنیت انسانی می شود. در عین حال، اگر حداقل شرایط برای امنیت بشر وجود نداشته باشد، توسعه انسانی دشوار است (Jolly, et al, 2007: 457-472).

حوزه امنیت انسانی می تواند به عنوان یک بستر ایمن، حلقه اتصال بین مفهوم امنیت تجاری و امنیت زیستی جهت تحقق توسعه انسانی مطرح بشود. طبیعتاً مفاهیمی چون، امنیت زیست محیطی، امنیت نظامی و توسعه بهداشت به عنوان مفاهیمی از امنیت انسانی در تحقق توسعه انسانی مفید اند اما در این تحقیق تمرکز بر عنصر امنیت اقتصادی به ویه امنیت تجاری است. حال آنچه که می تواند به طور جدی و در یک نسبت طولی، امنیت تجاری و در امتداد آن امنیت اقتصادی و نیز امنیت انسانی را تهدید کرده و مسیر تحقق توسعه انسانی را با چالشی از جنس اقتصادی روبه رو سازد، عدم محافظت دقیق از داده های اطلاعات تجاری است. بنابراین چنانچه سرقت از مالکیت معنوی را به عنوان یک مسأله امنیتی در نظر بگیریم، این امر به توجیه نظارت و کنترل بیشتر بر اینترنت و توسعه آینده آن کمک می کند به شرط پذیرش غیر قانونی بودن سرقت از مالکیت معنوی در تمام سطوح (Deborah & Halbert, 2016:256-262). البته نباید فراموش کرد که نگرانی های امنیتی همیشه به تفکر، سیاست ها و شیوه های مرسوم توسعه، متوسل است. پس از جنگ جهانی دوم تمرکز اصلی بر حفظ امنیت دولت ملی استوار بوده است و بر اساس این فرض که توسعه در گام اول مبتنی بر رشد اقتصادی تعریف شده است، پیش شرط امنیت و صلح به حساب آمده و برعکس عدم توسعه نیز به عنوان عامل بی ثباتی و وقوع درگیری قلمداد گردیده است (Busumtwi, 2002:255-257). اما آنچه که می تواند به طور جدی امنیت تجاری و اقتصادی را به خطر بی اندازد در دو زمینه جدا قابل بررسی است:

زمینه اول: نقض امنیت تجاری به دلیل مشارکت شخصیت های حقیقی یا حقوقی خارجی در مالکیت شرکت های داخلی است که می تواند به خودی خود منجر به مشروعیت بخشیدن به برداشت از اطلاعات تجاری شرکت ها و انتقال آن به مراکز تجاری خارج از قلمرو ملی کشورها شده و در نتیجه نقض مالکیت معنوی ملی شرکت ها، به ویژه شرکت های فعال در زمینه تکنولوژی، توسعه فناوری و انرژی را فراهم آورد.

زمینه دوم: درز اطلاعات کلیدی شرکت های تجاری مانند، فرمول های ساخت محصولات، اطلاعات حساب های مالی، اطلاعات حقوقی و همچنین داده های مربوط به فناوری و تکنولوژی است. که این خود در محدوده مالکیت معنوی قابل بررسی است و اصلی ترین دلیل آن، عدم وجود زیرساخت های قضایی و قانونی در بسیاری از قوانین ملی است که امکان درز اطلاعات تجاری را افزایش داده و امنیت اقتصادی را به شدت تحت تاثیر خود قرار می دهد. اما آنچه که در این میان حائز اهمیت است، بررسی روشی کار آمد در راستای محافظت از داده های اطلاعاتی شرکت های تجاری است. رویکرد قابل بررسی در اینجا، توجه به اصل پیشگیری در مشارکت های اقتصادی و نیز محافظت از انتقال غیر قانونی داده های اطلاعاتی است که می تواند به عنوان حلقه اتساع بین شاخصه امنیت اقتصادی و امنیت انسانی در نظر گرفته شود. حال در ادامه به بررسی اصل مورد نظر می پردازیم.

۵. جایگاه اصل پیشگیری در تحقق امنیت تجاری

اصل پیشگیری، یک نگرش عام در مواجهه با این پرسش اساسی است که، هنگام برخورد با خطرات و آسیب های نامتوازن، بایستی چه تدابیری اندیشید؟ این نگرش که مبتنی بر مقابله با خطرات احتمالی است، در جنبه های مختلف زندگی اجتماعی انسان تسری پیدا کرده به نحویکه می توان حوزه های عملیاتی آن را در بخش هایی نظیر محیط زیست و تغییرات اقلیمی، تغذیه و بهداشت عمومی، حفظ منابع طبیعی و انرژی های فسیلی، اقتصاد و جامعه شناسی نوین مشاهده نمود. آنچه که در این تحقیق مد نظر است، رویکرد اصل پیشگیری در برخورد با تهدیداتی است که امنیت اقتصادی و نیز امنیت تجاری را به خطر می اندازد. در همین راستا نگرش جامعه بین المللی در خصوص اهمیت این اصل در ماده ۱۵ اعلامیه ریو در سال ۱۹۹۲ نمایان می گردد، آنجا که این ماده به روشنی بیان می دارد: «در مواجهه با خسارت های تهدید کننده و جبران ناپذیر نباید به بهانه فقدان روش های قابل اطمینان، بررسی معیار های اثربخش را در ممانعت از افت بازار به تعویق انداخت.»

آنچه که امروزه منجر به بروز نگرانی در حوزه روابط اقتصادی شده است، بیشتر به مقوله امنیت اقتصادی و تجارت آزاد مرتبط است. جریان جهانی سرمایه گذاری مستقیم خارجی موسوم به (FDI)^۱ به نحو فزاینده ای از طریق سیاست های غربالگری، منجر به کاهش سرمایه گذاری

1. Foreign Direct Investment (FDI)

خارجی شده است. در دوران کنونی شاهد عزیمت از جریان آزادسازی بازارهای جهانی سرمایه که از اواخر قرن بیستم و اوایل قرن بیست و یکم به شدت جریان داشت، به محافظه کاری در مواجهه با جذب سرمایه گذاری خارجی از سوی دولت ها هستیم. تنها در سال ۲۰۱۸ معاملات گمرکی که حدود ۱۱ درصد از کل (FDI) جهانی را به خود اختصاص می داده است، به دلیل مداخله دولت ها مبتنی بر نگرانی های پیرامون امنیت، با شکست مواجه شده است (UNCTAD, 2019). تحول در رویکرد دولت ها هنگام مواجهه با دغدغه های امنیتی در مناسبات اقتصادی و تجاری بین المللی، نتایج مهمی در بخش انرژی، تولیدات صنعتی و نیز مبانی مالکیت فکری داشته است. به طور مثال در بخش انرژی این رویکردهای محافظه کارانه بیش از پیش نمایان شده حتی اگر در مسیر اکتشاف، تولید و تأمین تجهیزات و همچنین حفاظت از زیر ساخت های انرژی، در گذشته محدودیت های جدی در مسیر سرمایه گذاری، نوع مالکیت و نیز صدور مجوزهای بی شمار قرار داشته بود اما این محدودیت ها امروزه تشدید شده است. البته نباید فراموش کرد که رویکرد غربالگری سرمایه گذاری خارجی مبتنی بر پارامترهای امنیت ملی، موضوع جدیدی نبوده و در کنار آن مکانیزم های مختلفی برای کنترل فروش شرکت های داخلی به شخصیت های حقوقی خارجی به ویژه در بخش های حساس در طول قرن بیستم استفاده شده است.

اما رویکرد محافظه کارانه دولت ها در دوران کنونی در ارتباط با توسعه اقتصاد بین الملل تنها به رویکردهای کلی در اعطای مجوز سرمایه گذاری مستقیم، محدود نشده بلکه محافظت از داده های اطلاعات تجاری و جلوگیری از درز آن ها از اولویت های جدی دولت ها به حساب می آید. به دلیل توسعه فضای مجازی و عرصه وب، تهدیدات اقتصادی، شکلی تازه پیدا کرده که می توان از آن با عنوان حملات سایبری یاد کرد. امنیت داده های تجاری و نیز مالکیت معنوی از جمله ضروریات اقتصاد چند وجهی کلان در جامعه بین المللی است. اندیشه مبتنی بر اصل پیشگیری، امروزه در مواجهه با حملات سایبری و جلوگیری از درز اطلاعات تجاری خود را نمایان ساخته است. فرایند اجرای اصل پیشگیری با هدف تحقق امنیت تجاری نیاز به مشارکت بین المللی دارد. این مشارکت به طور یکپارچه تاثیرات گسترده ای بر فرایند حمایت از داده ها و رژیم های حفظ حریم خصوصی شخصیت های حقوقی مانند شرکت های تجاری را بر قوانین تجارت همسوی با فضای مجازی، برجسته می کند. دولت ها سعی بر آن دارند تا با تأکید بر

اصل پیشگیری، به جرم انگاری کیفی در محدوده درز اطلاعات تجاری مبادرت کرده تا هرچه بیشتر از وقوع آن جلوگیری نمایند.

آنچه که در این مسیر می تواند به عنوان یک دست آورد مهم مبتنی بر اصل پیشگیری در تحقق امنیت تجاری و محافظت از داده ها اطلاعاتی به حساب آید، استفاده از رویکرد کیفی در برخورد با جرایم حاصل از حملات سایبری در قالب قوانین نرم حقوق بین الملل است که می توان انعکاس این روش را در نسخه های آینده دستورالعمل های OECD^۱ برای شرکت های تجاری در نظر گرفت. و همانطور که در اصل دهم از «اعلامیه ریو» بیان شده است: حتی دولت ها می توانند نام شرکت هایی را که در فرایند حفظ اسرار تجاری تمهیدات لازم را رعایت نکرده اند و یا شرکای تجاری که مالکیت معنوی شرکت های دیگر را نقض کرده اند، منتشرنمایند که این خود می تواند در اجرای اصل پیشگیری جهت تحقق امنیت تجاری مفید باشد.

۵-۱. اصل پیشگیری و مکانیزم غربالگری سرمایه گذاری خارجی در حوزه فن آوری

آنچه که امروزه در فرایند غربالگری مبتنی بر اصل پیشگیری قابل توجه است، این است که نگرش جوامع توسعه یافته به سمت ممانعت از به شراکت گزیدن چهره های فعال در عرصه فن آوری است زیرا رقابت بین قطب های فن آوری در جهان اقتضا دارد تا امکان مشارکت در فرایند تحقیق و توسعه این مراکز تکنولوژی محافظت شده و حتی با عناصر قانونی مشارکت در سهام داری این شرکت ها، توجیه قانونی برای درز اطلاعات فراهم نیاید. این نگرش دقیقاً به مانند سیاست های غربالگری در صنایع مربوط به انرژی جریان دارد. به طور مثال، می توان به نگرش پیشگیرانه در خصوص تعمیرات و بروز رسانی سیستم CFIUS^۲ در ایالات متحده آمریکا در اواخر دهه ۱۹۸۰ اشاره کرد که در آن به دلیل نگرانی در مورد انتقال فناوری از طریق سرمایه گذاری شرکت های ژاپنی در مراکز فن آوری ایالات متحده آمریکا، با رویکرد غربالگری محدود گردید (Alvarez, 1989: 131). و اما امروزه مکانیزم های غربالگری در ایالات متحده آمریکا و اتحادیه اروپا به ویژه در مقابل کشور هایی چون ژاپن و کره جنوبی، به شکل فزاینده ای نشانگر بازگشت سیاست هایی است که بر رقابت تکنولوژیک تأکید دارند. به ویژه در حوزه هایی از فن آوری که بیشتر به صنایع نظامی و مصارف صنعتی حساس مرتبط اند (Mori, 2019: 77-120).

1. Organisation for European Economic Co-operation

2. The Committee on Foreign Investment in the United States (CFIUS)

آنچه که در این میان نباید نادیده گرفت، رویکرد پیشگیری از انتقال تکنولوژی و فن آوری است. البته این خود می تواند به پیشرفت مراکز علمی کشورها کمک کرده و با اتکای بر دانش بومی، زمینه های توسعه مترقیانه را در پیش گرفت اما به لحاظ حقوقی لاقبل در دوران کنونی، برای حفاظت از داده های فن آورانه و تکنولوژیک، ضرورت دارد تا مبتنی بر اصل پیشگیری، سیاست های غربالگری را به اجرا گذارد. در مقایسه با بخش انرژی و محافظت از درز اطلاعات تجاری در بخش صنایع انرژی، امروزه پیشگیری و محافظت از داده های اطلاعاتی مبتنی بر سیاست غربالگری در بخش فن آوری جریان دارد. در همین راستا می توان به دستور رئیس جمهور وقت آمریکا در سال ۲۰۱۷ اشاره کرد، آنجا که ایشان امکان دسترسی شرکتی مستقر در ایالات متحده آمریکا به اطلاعات تجاری (دستگاه های نیمه هادیتر مشبک) که از سوی دولت چین در قالب سرمایه گذاری مشترک تامین مالی می شد، را مسدود کرد. همچنین در سال ۲۰۱۸ فروش دستگاه تراشه ساز Qualcomm به شرکت Broadcom که در حقیقت یک شرکت با سرمایه قالب از سوی کشور سنگاپور بود نیز به همان ترتیب با محدودیت های جدی روبه رو گردید. البته غربالگری مبتنی بر اصل پیشگیری تنها در زمینه دانش و فن آوری محدود نبوده بلکه در ایالات متحده آمریکا بررسی های محدود کننده بر فناوری اطلاعات، فناوری مالی و نیز علوم مرتبط با تولید داروهای پزشکی نیز توسعه پیدا نموده است (Zimmerman, 2019: 1304-1267). امروزه دولت ها به دلیل درز اطلاعات تجاری و مالکیت معنوی شرکت های فعال در زمینه فن آوری و انرژی، به شدت نسبت به مشارکت در مالکیت شرکت های خارجی در این حوزه دچار تردید شده و سعی در ایجاد محدودیت های جدی در این مسیر دارند. شاید بتوان در این باره مبتنی بر اصول موجود در اقتصاد بازار آزاد، انتقاد جدی را بر اعمال محدودیت دولت ها در زمینه سرمایه گذاری شرکای خارجی در طرح های مربوط به فن آوری را مطرح نمود اما در پاسخ باید دانست که حفاظت از داده های مالکیت معنوی به محدوده منافع ملی و نیز حوزه امنیت ملی جوامع ارتباط پیدا می کند که این خود تأثیر مستقیمی بر مفهوم امنیت انسانی در جوامع امروزی دارد، که این خود اعمال اصل پیشگیری مبتنی بر فرایند غربالگری سرمایه گذاری خارجی را توجیه کرده و آن را مشروع می نماید. چگونه می توان انتظار داشت که دولت ها هنگام تزریق سرمایه به شرکت های دانش بنیان برای توسعه فن آوری و زیرساخت های تکنولوژیک، از درز اطلاعات این مجموعه ها حراست نکرده و بستر انتقال میلیاردها دلار مالکیت معنوی را به خارج از کشور با تکیه بر شعار اقتصاد بازار آزاد، مهیا کنند؟

۵-۲. اصل پیشگیری و دفاع سایبری

قبل از بررسی دفاع سایبری مبتنی بر اصل پیشگیری، لازم است هجوم سایبری را مورد ارزیابی قرار دهیم. هجوم سایبری زمانی اتفاق می افتد که به حوزه اطلاعات خصوصی یک شرکت مانند: داده های اطلاعات مالی، حساب های بانکی، اطلاعات موجود در بخش تحقیق و توسعه، فرمول های حساس تولید کالا، اطلاعات مربوط به اسناد تجاری و حقوقی، اطلاعات پیرامون نشر و مالکیت معنوی آثار فرهنگی و علمی و... که به نوعی در طبقه بندی حریم خصوصی شخص حقوقی قابل اعمال است، به شکل غیر قانونی و بدون اخذ رضایت از مالکین معنوی و حقیقی آن، دست اندازی صورت پذیرد. در طول دهه های گذشته، این تأکید و محافظت مبتنی بر رویکرد موجود در اصل پیشگیری از سرقت داده های اطلاعاتی در حوزه نشر و چاپ اتفاق افتاده است که به نوبه خود به قانون حفظ حریم خصوصی داده ها کمک کرده است، به نحوی که از آموزه های حفظ حریم خصوصی برای کمک به جنبه های حق چاپ استفاده شده است (Lee A & Bygrave, 2014: 78).

اما از نظر فنی، دفاع سایبری مبتنی بر اصل پیشگیری از نقض امنیت تجاری، دفاع در برابر نفوذ، سرقت و جاسوسی چه به صورت فعال چه غیر فعال طبقه بندی می شود. اگرچه که متولی قانونی و حقوقی در راستای دفاع سایبری، دولت ها هستند اما عدم موفقیت دولت ها در غرب بر سر حراست از داده های اطلاعاتی، بسیاری از تحلیلگران، محققان و سیاستگذاران حوزه فضای مجازی و اقتصاد آنلاین را بر آن داشت که به مشارکت بخش خصوصی در این زمینه تأکید نمایند، به نحویکه شرکت ها بایستی خود را در وضعیت دفاع فعال از داده های اطلاعاتی، نگهدارند (Rosenzweig, 2017).

بنابراین بسیار مهم است تا جنبه تحقق محافظت از داده های اطلاعاتی را مبتنی بر اصل پیشگیری در ساز و کار مقدماتی تأسیس شرکت پیش بینی نموده و دولت ها در هنگام صدور مجوزهای قانونی تحقق زیرساخت های محافظتی را مطالبه نمایند. اعطای چنین نقشی به بخش خصوصی می تواند منجر به تحقق دفاع شخصی در برخورد با حملات سایبری شده و انتقال این رسالت از دولت به شرکت های خصوصی می تواند امکان نظارت بی حد و اندازه دولت در حقوق خصوصی را کاهش دهد. البته انتقال مسؤلیت مبتنی بر اصل پیشگیری از دولت ها به بخش خصوصی، رافع مسؤلیت نهادهای قضائی کشورها برای ایجاد بستر های حقوقی نمی باشد. بدین معنی که بایستی به موازات رعایت پروتکل های حفاظتی توسط

شرکت‌ها، نهادهای قانونگذاری و دستگاه‌های قضائی کشورها به تنظیم قوانین و مقرر کارآمد در فرایند امکان‌جبران خسارات ناشی از درز اطلاعات تجاری شرکت‌ها مبادرت ورزند. در همین راستا، حمایت قضایی موجود در ایالات متحده آمریکا از اعطای این نقش به بخش خصوصی قابل تأمل است. قانون دفاع از اسرار تجاری موسوم به (DTSA)^۱ با ایجاد بستر حقوقی و قضایی جهت جبران خسارت‌های ناشی از دسترسی غیرقانونی به اسرار تجاری، توسعه داده‌های تجاری شرکت‌های خصوصی را از حمایت قانونی به‌رمنده نموده است. این امر به دادگاه فدرال اجازه می‌دهد که برای جلوگیری از سوء استفاده قطعی و حقیقی از داده‌های تجاری شرکت‌ها، حکم دادخواست صادر کند (Alan Charles & Vivek K, 2018: 376-383). همچنین امروزه در بسیاری از مکانیزم‌های قضائی کشورها، در ارتباط با حفاظت از مالکیت معنوی، استانداردهای جدید و کارآمدی (که البته بیشتر تحت تأثیر سازوکارهای موجود در سازمان تجارت جهانی/ WTO) تنظیم شده‌اند که با جدیت تمام، حفاظت از مالکیت معنوی مورد توجه قرار گرفته است (Yujing Liu, 2018: 68). در همین راستا کشور هندوستان معتقد است که فرایند یکپارچه سازی محافظت از داده‌های تجاری به ویژه تجارت بین‌المللی کالا، بایستی تحت نظارت و سیاست‌گذاری سازمان تجارت جهانی صورت گرفته و حتی وزیر امور خارجه این کشور آن گونه که در سال ۲۰۱۹ بیان می‌دارد، معتقد است که امروزه، «داده‌های اطلاعاتی، شکل جدیدی از ثروت محسوب می‌شوند». بنابراین ضرورت دارد تا در راستای محافظت از آن، سازمان‌های بین‌المللی به ایجاد سازوکارهای واحد مبادرت ورزند. آنچه که بدیهی است این حقیقت است که سهم اقتصاد مبتنی بر سرمایه حاصل از مالکیت معنوی، از دهه ۸۰ میلادی قرن بیستم به طرز چشمگیری رشد کرده است. در همین راستا ارزش کل دارایی معنوی ایالات متحده آمریکا در سال ۲۰۱۲، ۵/۵ تریلیون دلار معادل ۳۹ درصد از تولید ناخالص داخلی این کشور تخمین زده شده است و این بدان معنا است که بخش مربوط به مالکیت معنوی، حتی اگر با گزاره‌های اقتصادی کلان ارزیابی گردد، به صورت قابل توجهی رشد کرده و نیز به رشد خود ادامه می‌دهد (U.S. Econ, 2016:150-177). بر همین اساس در گزارشی در ماه مه سال ۲۰۱۳ از سوی کمیسیون سرقت از دارایی معنوی ایالات متحده آمریکا بیان شده است که خسارت سالانه بر پیکره اقتصاد این کشور به دلیل عدم محافظت دقیق از داده‌های تجاری و نیز سرقت این داده‌ها حدود ۳۰۰ میلیارد دلار معادل ۲٪ از سهم تولید

1. Defense Technology Security Administration (DTSA)

ناخالص داخلی این کشور و نیز امکان اشتغال زایی برای ۲۰۱ میلیون نفر در سال است (Blair & Huntsman, 2013: 175).

حجم بالای این خسارات، تأثیر مستقیم بر پیکره امنیت ملی و نیز امنیت انسانی جوامع داشته به نحویکه جبران خسارات ناشی از این فرایند سال ها کشورهای صنعتی و در حال توسعه را تحت تأثیر خود قرار می دهد. میزان آسیب پذیری جوامع کم تر توسعه یافته به دلیل عدم توسعه زیرساخت های تکنولوژیک به مراتب بالا تر از کشورهای توسعه یافته است.

نتیجه گیری

از آنجاییکه امروزه، مفهوم امنیت انسانی از سوی جامعه بین المللی به عنوان یکی از اساسی ترین ابزارهای تحقق توسعه پایدار به شمار می آید و جامعه مدنی بین المللی به عنوان اکوسیستمی فعال و در هم تنیده از منافع سیاسی، فرهنگی و اقتصادی مطرح است، دولت-ملت ها سعی دارند تا با تحقق مفهوم امنیت ملی پایدار، از منافع ملی خود محافظت کرده و سهم قابل توجهی از فرایند توسعه مبادلات بین المللی را به خود اختصاص دهند. بر همین اساس در این تحقیق مشخص شد که:

اول اینکه: مفهوم امنیت انسانی تنها به رویکرد زیست محیطی و محافظت از منابع طبیعی در آن محدود نمی گردد بلکه امروزه به دلیل توسعه روابط اقتصادی و نیاز متقابل جوامع به یک دیگر، امنیت انسانی مستلزم تحقق امنیت اقتصادی است. زیرا پایداری در بهره مندی از ثبات اقتصادی منجر به بهبود معیشت انسان در جامعه می شود که این خود پایداری در زیست اجتماعی را محقق می سازد.

دوم اینکه: توسعه روابط تجاری بین المللی و نیز گسترش رقابت دولت ها در اقتصاد بازار آزاد که خود بر توسعه علم و فن آوری استوار است، مستلزم محافظت از داده های تجاری و مالکیت معنوی شرکت ها است. از همین رو، تحقق امنیت اقتصادی موکول و متوقف بر تحقق مفهوم امنیت تجاری است.

بر این اساس، در این تحقیق اثبات گردید که امروزه تحقق مفهوم امنیت ملی تنها در کاهش آسیب پذیری نظامی و زیست محیطی خلاصه نمی شود بلکه محافظت از داده های تجاری و مالکیت معنوی شرکت ها در حوزه فن آوری به جهت تحقق امنیت تجاری یک ضرورت ملی است. از این رو مسؤولیت تحقق مفهوم امنیت تجاری با دولت ها است زیرا تحقق مفهوم امنیت

اقتصادی ذیل مفهوم امنیت ملی قرار می‌گیرد و دولت‌ها بایستی به عنوان متولی اصلی در محافظت از داده‌های جمعی تجاری در نظر گرفته شوند. اما این بدان معنی نیست که بخش خصوصی در راستای حفاظت از داده‌های تجاری و مالکیت معنوی هیچ مسؤولیتی ندارد. باید دانست، مسأله اصلی این نیست که مسؤولیت محافظت از داده‌های تجاری با دولت است یا با بخش خصوصی بلکه مسأله اصلی، فرایند قانونگذاری است که بایستی قانونگذار مبتنی بر اصل پیشگیری، به محافظت قانونی از داده‌های تجاری و پر کردن خلأهای مشروع در این زمینه مبادرت ورزد.

بر همین مبنا محوری‌ترین نوآوری این مقاله آن است که جهت افزایش توان محافظت قانونی از مالکیت معنوی شرکت‌های فن‌آوری و کاهش میزان درز اطلاعات تجاری بنگاه‌های اقتصادی به دلیل خلأهای قانونی، روش غربالگری در سرمایه‌گذاری مستقیم خارجی ارائه می‌شود تا شرکای خارجی نتوانند با سوءاستفاده از سکوه‌های پنهان در شراکت، به انتقال داده‌های تجاری و فن‌آوری به خارج از مرزهای ملی مبادرت ورزند. این امر بدیهی است که بدون بالابردن توان محافظتی در مقابل حملات سایبری نمی‌توان به طور کامل از داده‌های تجارت جمعی محافظت کرد. بنابراین، رویکردهای قانونی به حملات سایبری و تأثیر آن بر تحقق امنیت جمعی می‌تواند موضوع تحقیق در آینده باشد تا از رهگذر آن بتوان بیش از پیش به تأثیر تحقق امنیت اقتصادی در تحقق مفهوم امنیت انسانی دست یافت.

فهرست منابع

- Alvarez, Jose E. (1989), "Political Protectionism and United States International Investment Obligations in Conflict: the Hazards of exon-florio Va. J". **Int. Law**, 30.
- Braithwaite, John & Drahos, Peter (2000), **Global Business Regulation**, Cambridge University press.
- Busumtwi-Sam, J. (2002). "Development and Human Security: Whose Security and from what?" **International Journal**, 57(2): 2002; 253-272
- Bygrave, Lee A. (2014), "Data Privacy Law", **An International Perspective**, 13(20 14).
- Charles Raul, Alan & Mohan, Vivek K. (2018), "United States, in The Privacy, Data Protection and Cybersecurity Law", **Review** 376, 383.

- Chiara, Gaido (2017), "The Trade Secrets Protection in U.S. and in Europe": A Compar-ative Study, **Revista La Propiedad Inmaterial**, 24(2) 129, 132.
- Debora J. Halbert (2016). "Intellectual Property Theft and National Security: Agendas and assumptions", **journal The Information Society**. 32(4) 256, 262.
- Dralle, Tilman Michael (2018), "Ownership Unbundling and Related Measures in the EU Energy Sector": **Foundations**, the Impact of WTO Law and Investment Protection Springer.
- Evan Zimmerman. (2019), "The Foreign Risk Review Modernization Act: How CFIUS became a Tech Office", **Journal Berk. Technol. Law J.**, 34 (4), pp. 1267-1304.
- Ezati, M & Dehghan, M, (2008), **Economic Security in Iran**, Research Center, Office of Economic Studies, Iran, Tehran.
- Grigoreva, Ekaterina & Fesina Elena(2013), "Economic Security as a Condition of Institutional Support of Economy Modernization", **World Applied Sciences Journal**, vol. 31, no. 5, pp. 940-948.
- Howg, Jason (2017), **Unique Trade Secret License Agreement Features**, Lexol-ogy Mar. 31.
- Jolly, R., & Basu Ray, D. (2006), **National Human Development Reports and the Human Security Framework**, New York: Human Development Report Office, UNDP.
- Kafshgar, J, (2014), **Economic Security**, Website of Baqer Al-Uloom Research Institute, Iran.
- Kanbur, Ravi (2001), Economic Policy, Distribution and Poverty: The Nature of Disagreements", **World Development**, 1083-1094.
- Litvinenko A.N., (2013), "Economic and National Security" : the Problem of Concepts Correlating // Scientific and Technical statements, S.-Petersburg State Polytechnic University, **Economic sciences**, No 3 (173), pp. 9-15.
- Liu, Yujing (2018), "Prepare for more Cyberattacks Involving Extortion this Year", Hong Kong Information Security Watchdog warns, **South China Morning Post** (Jan. 18).
- Mark Wu , (2018), **Export Policies, Technology Transfer Policies, and Investment Reviews, How States Compete in the era of Global High-tech Value Chains**, National Security-related Screening Mechanisms for Foreign Investment: an analysis of Recent Policy Developments(2019). https://unctad.org/en/PublicationsLibrary/diaepcbinf2019d7_en.pdf.

- Morius, Satoru (2019), Technological Competition with China: the Military, Industrial and Digital Network Dimensions Asia Pac. **Rev.**, 26 (1) , pp. 77-120.
- Peter K. Yu,. (2015), "Trade Secret Hacking, online Data Breaches, and China's Cy-berthreats", **Cardozo Law Review de novo** 130, 133-134 .
- Sauvant , Karl P. (2009), FDI Protectionism Is on the Rise" . **Policy Research Working PapersThe World Bank**, 10.1596/1813-9450-5052
- Shin-yi Peng, Han-Wei Liu, Ching-Fu Lin (2018), In **Governing Science And Technology Under the International Economic Order**, Edward Elgar Publishing (2018), pp. 90-113.
- United Nations Human Development Reports (2011), **Human Development Reports**, New York: United Nations Development Programme, Accessed November 1.
- Xiong, Ping (2016), "China's Approach to Trade Secrets Protection, Is a Uniform Trade Secrets Law in China needed?", in**The Internet and the Emerging Importance of new Forms of Intellectual Property**, 251, 252; 256-262 (Susy Rebecca Frankel & Daniel J. Gervais, ed., 2016).