

A Comparative Study of the Electronic Evidence in Criminal Justice Systems of Iran and China

* Babak Pourghahremani

Associate Professor, Department of Criminal Law and Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran
b.pourghahremani@yahoo.com

Reza Ghaderi

PhD Student, Department of Criminal Law and Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran

DOI: 10.30495/CYBERLAW.2022.692009

Keywords:

Electronic evidence, credibility of electronic evidence, data seizure, data collection, criminal justice system of Iran and China.

Abstract

Background and Objective: With expansion of cyberspace, crimes in this area have also spread. The need for credibility, seizure and collection of electronic evidence has been considered in various criminal justice systems. The purpose of this article is to comparatively study and analyze the position of electronic evidence in the criminal justice systems of Iran and China.

Method: The present research employs a descriptive-analytical method in reaching its objectives. The rules and regulations governing electronic evidence in China and Iran have been studied and comparatively examined.

Findings: Investigating cybercrime requires the seizure, collection and credibility of electronic evidence in the trial process. The laws and regulations of Iran and China have dealt with these issues separately and have provided solutions for criminal prosecution by criminalizing cybercrime.

Results: The criminal systems of Iran and China have adopted different regulations and laws with regard to collection, seizure and credibility of the electronic evidence according to their own needs in the society. The legal system of China is more developed than Iran as far as its technical and specialization are concerned. The legal system of Iran, in its turn, follows a human rights approach of the same and attempts at restricting the authority of the justice administration law enforcement agents by stating their duties and responsibilities. Both of the systems use police force as the responsible body for collecting, seizure and credibility of the electronic evidence.



This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license:

(<http://creativecommons.org/licenses/by/4.0/>)

مطالعه تطبیقی ارزیابی ادله الکترونیکی در نظام عدالت کیفری ایران و چین

دکتر بابک پور قهرمانی

دانشیار گروه حقوق کیفری و جرم شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران
b.pourgharamani@yahoo.com

رضا قادری

دانشجوی دوره دکتری گروه حقوق کیفری و جرم شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران

تاریخ پذیرش: ۱۸ خرداد ۱۴۰۱

تاریخ دریافت: ۰۴ اسفند ۱۴۰۰

چکیده

زمینه و هدف: همزمان با گسترش فضای مجازی، جرایم این حوزه نیز گسترش پیدا نموده است. لزوم استنادپذیری، توقیف و جمع آوری ادله الکترونیکی در نظام های مختلف عدالت کیفری مورد توجه واقع شده است. هدف این مقاله مطالعه تطبیقی ادله الکترونیکی در نظام عدالت کیفری ایران و چین می باشد. روش: این پژوهش از نظر تدوین توصیفی تحلیلی می باشد. قوانین و مقررات ادله الکترونیکی در چین و ایران مورد مطالعه و به صورت تطبیقی مورد بررسی قرار گرفته است.

یافته ها: رسیدگی به جرایم فضای مجازی نیازمند توقیف، جمع آوری و استنادپذیری ادله الکترونیکی در فرایند دادرسی می باشد. قوانین و مقررات ایران و چین به صورت مجزا به این موضوعات ورود کرده و با جرم انگاری جرایم سایبری در راستای رسیدگی کیفری راه کارهایی را ارائه نموده است.

نتایج: نظام های حقوقی ایران و چین در زمینه جمع آوری، توقیف و استنادپذیری مقرراتی به فراخور جامعه خود دارند. نظام حقوقی کشور چین در زمینه فنی و تخصصی پیشرو تر از مقررات ایران می باشد. در مقابل نظام حقوقی ایران رویکردی حقوق بشری به موضوع دارد و با بیان وظایف ضابطان دادگستری سعی در تحدید حدود اختیارات ایشان است، هر دو نظام حقوقی از پلیس به عنوان مسئول جمع آوری و توقیف و استنادپذیری استفاده نموده اند.

کلید واژگان: ادله الکترونیکی، استناد پذیری ادله الکترونیکی، توقیف داده ها، جمع آوری داده ها، نظام عدالت کیفری ایران و چین

مقدمه

بشر در طول دوران رشد و تکامل خود دوره‌های مختلفی را تجربه کرده است، و هر دوره به جهت بروز و ظهور پدیده‌ای جدید به نام آن نام گذاری شده است، مانند عصر صنعتی شدن. عصر حاضر به جهت گسترش ابزارهای فناورانه دیجیتالی به عصر دیجیتال شهرت یافته است. از یک سو پیشرفت چنین فناوری‌هایی، رفاه زیادی را برای زندگی مردم به ارمغان آورده است، از سوی دیگر، زندگی مردم را با چالش‌هایی جدی مواجه نموده و در مواردی نیز دچار مشکل کرده است. چالش عصر حاضر ظهور جرایم جدید در بستر فضای سایبر می‌باشد، که به جرایم سایبری یا جرایم رایانه‌ای شهرت یافته‌اند. با اینکه نسبت تعداد جرایم سایبری در پرونده‌های جنایی از کشوری به کشور دیگر متفاوت است، اما غیرقابل انکار است که تقریباً تمام کشورها در عصر اینترنت به نوعی با جرایم سایبری درگیر هستند. در دادرسی‌های کیفری، یکی از مرحله‌های اصلی برای کشف حقیقت بررسی ادله اثبات جرم می‌باشد و در این بین ادله‌های الکترونیکی رکن اساسی پرونده‌های جرایم سایبری می‌باشند. بیشتر کشورها برای سر و سامان دادن به فضای سایبر، مقرراتی را به منظور مقابله با جرایم سایبری و ادله موجود در قالب ادله‌های الکترونیکی، به تصویب رسانده‌اند. هنگام رسیدگی به پرونده‌های کیفری به ویژه پرونده‌های جرایم سایبری، تاکید مضاعف بر ادله‌های الکترونیکی و بررسی مقررات موجود در خصوص آنها، در حوزه‌های مختلف قضایی از اهمیت بسزایی برخوردار است تا اطمینان حاصل گردد که استناد به این ادله‌ها برای مسائل فعلی نظام حقوقی و جامعه مناسب هستند. نظام حقوقی ایران ادله اثبات دعوا را در قانون مدنی تعریف نموده است، که به طور خلاصه می‌توان گفت: دلیل عبارت از هر وسیله قانونی است که مقامات قضایی را در کشف حقیقت و حصول اقرار و جدانی و اتخاذ تصمیم یاری بخشد. با ابتنا بر این ادله الکترونیکی عبارت است از هر گونه داده الکترونیکی که در راستای اثبات دعوا در محاکم قضایی به آن استناد گردد. با توجه به جدید بودن ادله الکترونیکی در دنیا می‌بایست تحقیقات علمی در راستای شناخت ابعاد آن صورت گیرد تا با استفاده از مطالعات تطبیقی بتوان از یافته‌های کشورهای پیش رو در این زمینه استفاده کرد. از زمانی که کشور چین به اینترنت متصل گردید مقام‌های چینی واکنش‌های فعالی به این موضوع نشان دادند و سعی بر نظام‌مند نمودن آن و همچنین استفاده از ادله الکترونیک در پرونده‌های جنایی داشتند. در جمهوری خلق چین بیش از ۴۸۰۰۰ پرونده با موضوعات جرایم سایبری در دادگاه‌های چین بین سالهای ۲۰۱۶ تا ۲۰۱۸ تشکیل گردیده است که در این پرونده‌ها نیز موضوع مهم ادله الکترونیکی مطرح شده است. موضوع مهمی که در قوانین کشور چین نیز به چشم می‌خورد عدم تکافوی قوانین موجود در خصوص چالش‌های ادله الکترونیکی می‌باشد. بر همین اساس کشور چین به جهت پیشرفت فزاینده در زمینه فضای سایبر و ابزارهای فناورانه مرتب با این فضا دارای ظرفیت بالایی برای مطالعه در این خصوص می‌باشد به همین جهت نگارندگان این کشور را برای بررسی تطبیقی در خصوص ادله الکترونیکی انتخاب نمودند. با توجه به تلاش‌های مسئولان ایران برای گنجاندن داده‌های الکترونیکی در نظام عدالت کیفری و قانون جرایم رایانه‌ای و آیین‌نامه اجرایی این قانون و گسترش جرایم رایانه‌ای و لزوم رسیدگی به آنها، این مقاله بر مقررات حاوی ادله الکترونیکی در ایران و چین تمرکز داشته و به دنبال پاسخ به این سوال است که از حیث مطالعه تطبیقی، ادله الکترونیکی در نظام عدالت کیفری ایران و چین چیست؟

۱ - مفهوم‌شناسی

در این بخش ابتدا مفاهیم ادله الکترونیکی و داده‌های الکترونیک را در دو بخش مورد بررسی قرار می‌دهیم. نخست ادله الکترونیکی را با تعریف ادله در نظام حقوقی ایران و الکترونیک به صورت جداگانه مورد تبیین قرار می‌دهیم. در بخش بعدی داده‌های الکترونیکی را تعریف نموده و به نظر قانونگذار را در این زمینه خواهیم پرداخت.

۱ - ۱ - ادله الکترونیکی

ادله در لغت جمع دلیل به معنای راهنمایان، حجت‌ها و برهان‌ها می‌باشد (معین، ۱۳۸۰: ۶۵) در زبان و ادب فارسی دلیل به معنای راهنما و رهنمون و نشان و علامت آمده است (شمس، ۱۳۹۰: ۲۸) در اصطلاح عرفی به چیزی گفته می‌شود که امری را اثبات نماید. برخی حقوقدانان با مد نظر قرار دادن اصطلاح عرفی در تعریف دلیل چنین می‌گویند: دلیل در اصطلاح عرف به چیزی اطلاق می‌شود که امر مجهولی را ثابت نماید یا عامل اثبات حقیقت امری است که مورد ادعا یکی از اصحاب دعوی و انکار دیگری باشد (مدنی، ۱۳۷۲: ۷). علمای حقوق، با عنایت به ماهیت و ارزش اثباتی دلایل، آنها را به اقسام مختلفی تقسیم نموده‌اند (امامی،

۱۳۷۰: ۱۲) در ماده ۱۹۴ قانون آیین دادرسی مدنی این طور آمده است «دلیل امری است که اصحاب دعوا برای اثبات یا دفاع از ادعا به آن استناد می‌کنند (کاتوزیان، ۱۳۸۸: ۴۲). همچنین قانون مدنی طی ماده ۱۲۵۸ ادله اثبات دعوی را در ۵ قسم یعنی اقرار، اسناد کتبی، شهادت، امارات و قسم بر شمرده است. و در ماده ۱۲۸۴ سند را چنین تعریف کرده است: سند عبارت است از هر نوشته که در مقام دعوی یا دفاع قابل استناد باشد. در حقوق کیفری تعریفی از دلیل ارائه نشده است و تنها در ماده ۱۶۰ قانون مجازات اسلامی مصوب سال ۱۳۹۲ قانون گذار به احصای ادله پرداخته است: ادله اثبات جرم عبارت از اقرار، شهادت، قسامه و سوگند در موارد مقرر قانونی و علم قاضی است. با این وجود در رویه قضایی ایران اگر چه در خصوص پذیرش ادله الکترونیکی تردیدهای فراوان وجود داشت. با تصویب قانون تجارت الکترونیک در سال ۱۳۸۲ ارزش اثباتی آن به عنوان دلیل مورد تایید قانونگذار ایران قرار گرفت. قانون تجارت الکترونیکی نیز در مواد ۶ تا ۱۲ به جایگاه و ارزش اثباتی ادله الکترونیک در قالب ادله پیام، پرداخته و در ماده ۴ اینگونه تعریف نموده است: هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فن‌آوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود. ماده ۱۲ به طور کلی بیان می‌دارد: اسناد و ادله ممکن است به صورت ادله پیام باشد، سر انجام با تصویب قانون جرایم رایانه‌ای در سال ۱۳۸۸ این نقیصه از لحاظ کیفری تا حدودی در کشور ما بر طرف شده است اما نمی‌توان آن را مجموعه کاملی جهت رفع مشکلات استناد به ادله الکترونیکی در ایران دانست. ماده ۵۰ قانون جرایم رایانه‌ای نیز بدون آنکه وصف خاصی برای محتوای حافظه رایانه در نظر بگیرد آن را با وجود شرایطی قابل استناد شناخته است.

در اصطلاح، ادله الکترونیک، اطلاعات و ادله‌های ارزشمند تحقیقاتی معنی شده‌اند که بر روی یک وسیله الکترونیکی ذخیره شده یا توسط آن انتقال ادله می‌شوند. بنابراین ادله الکترونیک در برگیرنده هر نوع ادله الکترونیکی است که می‌تواند مثبت امر حقوقی یا اثبات‌کننده وقوع جرم و یا فراهم‌کننده ارتباط بین جرم و قربانی آن یا جرم و عامل ارتكابی آن باشد. با عنایت به تعاریف صورت گرفته از دلیل و الکترونیک، تعریف از دلیل الکترونیکی با ترکیب این دو کار سختی نیست، بنابراین می‌توان گفت: هرگونه ادله یا نرم‌افزار یا سخت‌افزار الکترونیکی که بتواند اطلاعات ارزشمندی در راستای اثبات ادعا، دفاع، کشف جرم، یا استدلال قضایی به دست دهد، دلیل الکترونیکی محسوب می‌شود. بنا به تعریف جامع‌تر می‌توان گفت: ادله الکترونیکی عبارت است از اسناد و مدارک ثبت شده در سامانه‌های رایانه‌ای، اینترنت و اتوماسیون‌های اداری به عبارت دیگر، به اسناد و مدارک موجود در دنیای مجازی، ادله الکترونیکی گفته می‌شود. البته ادله الکترونیک به رایانه ختم نمی‌شوند و همه اطلاعات قابل کسب از دستگاه‌های الکترونیکی از جمله تلفن همراه، دوربین‌ها و غیره را شامل می‌شود، ملاحظه می‌گردد اسناد و مدارک ثبت شده در سامانه رایانه‌ای و سایر دستگاه‌های الکترونیکی را ادله الکترونیکی می‌نامند (شیرین زاده، ۱۳۹۴: ۵) دلیل الکترونیکی در معنی رایج و مصطلح عبارت است از هر ادله پیامی که اصحاب دعوا برای اثبات یا دفاع از مدعای خود به آن استناد می‌کنند (شهبازی‌نیا، ۱۳۸۹: ۲۰۸)

۱ - ۲- داده‌های الکترونیکی

جرایم سایبری برای اولین بار در سال ۱۹۹۷ رخ داد و از آن زمان، قانون کیفری جمهوری خلق چین برای رسیدگی به جرایم سایبری مورد استفاده قرار گرفت. در همان زمان، محققان چینی وقت و توجه زیادی را برای مطالعه ادله‌های الکترونیکی اختصاص دادند. در ابتدا، اصطلاح حقوقی مشخصی برای تبیین این ادله وجود نداشت تا آنکه امروز به این ادله، ادله‌های الکترونیکی گفته می‌شود، محققان از اصطلاحات ادله‌های الکترونیکی، ادله رایانه‌ای، ادله دیجیتال و ادله الکترونیکی به جای یکدیگر استفاده می‌کردند (لانگ و پی، ۲۰۱۶: ۴۰) با در نظر گرفتن ویژگی‌های ادله‌های الکترونیکی، بعضی از محققان اینگونه استدلال کرده‌اند که ادله‌های الکترونیکی را می‌بایست به‌عنوان بخشی از ادله فیزیکی و مستند یا ادله صوتی و تصویری در نظر گرفت، زیرا ادله‌های الکترونیکی فقط به‌عنوان ابزاری برای ذخیره‌سازی یا استنادپذیری این ادله مورد استفاده قرار می‌گیرند (کویی، ۲۰۰۷: ۵۱) در مقابل، محققان دیگری معتقدند که ادله‌های الکترونیکی باید به‌عنوان نوعی مستقل از ادله سنتی در نظر گرفته شوند و قوانین جدید متناسب با ادله‌های الکترونیکی باید وضع شود زیرا ادله‌های الکترونیکی ذاتاً دارای ویژگی‌هایی هستند که ادله‌های قبلی و سنتی فاقد آنها هستند (هاو، ۲۰۰۷: ۴۰) می‌توان دریافت که ادله‌های الکترونیکی، به‌عنوان یک پدیده نوظهور، نظر محققان علمی این

دوره را به خود جلب کرده بود، اما به علت عدم درک عمیق محققان از ادله‌های الکترونیکی، در یک تعریف محدودی خلاصه شد. با اینکه این ادله‌ها تنها انعکاس متفاوتی از نظایر خود در دنیای فیزیکی به شمار می‌آیند، ولی ویژگی‌های منحصر به فردی دارند که مستلزم قواعد و تدابیر جدیدی هستند. در زیر به بعضی از نقاط قوت و نقاط ضعف ادله‌های الکترونیکی اشاره می‌شود.

از جمله ویژگی‌هایی که شاید بتوان آنها را نقاط قوت ادله‌های الکترونیکی نسبت به اطلاعات فیزیکی برشمرد، عبارت‌اند از (کپسی، ۱۳۸۶: ۱۹)

- ۱- از داده‌های الکترونیکی می‌توان کپی برداری کرد، به نحوی که تنها راه تفکیک اصل از کپی، مراجعه به یک سری داده‌های ثبت شده خاص در سیستم رایانه‌ای مورد نظر است.
 - ۲- به لحاظ قرار داشتن ادله‌ها در قالب انعطاف‌پذیر الکترونیکی و همچنین امکان کپی برداری دقیق از آنها، به راحتی می‌توان هرگونه تغییر و اصلاح را در نسخه‌های کپی، همانند نسخه اصلی انجام داد و اصل سند را محفوظ داشت.
 - ۳- هرگونه تغییر و اصلاح انجام شده در داده‌ها، در فایل‌های جداگانه‌ای به ثبت می‌رسد؛ به همین دلیل، می‌توان با به کارگیری ابزار و برنامه‌های بسیار متنوعی که برای این کار طراحی و تولید شده‌اند، به موارد تغییر یافته پی برد.
 - ۴- از بین بردن داده‌های الکترونیکی مشکل است. آنچه که ما در واقع امر به هنگام پاک کردن ادله‌ها انجام می‌دهیم، از بین بردن آنها نیست، بلکه غیر قابل دسترس کردن آنهاست. آنها در فضاهای راکد دیسک‌های ذخیره باقی می‌مانند، که با به کارگیری نرم‌افزارهای ویژه می‌توان بسیاری از آنها را بازیابی کرد.
 - ۵- چنانچه ادله‌های رایانه‌ای از یک سیستم رایانه‌ای خارج و در فضای سایبر رها شوند، کپی‌های آنها در بسیاری از نقاط ذخیره خواهند شد. این وضعیت باعث می‌شود، از یک سو امکان از بین رفتن ادله به حداقل برسد و از سوی دیگر با استناد به سوابق الکترونیکی بیشتر و متنوع‌تر، امکان محکمه پسند بودن آنها افزایش می‌یابد.
- در مقابل، این ادله‌ها نقاط ضعف انکارناپذیری دارند، از جمله:

- ۱- مهم‌ترین ایراد این نوع اطلاعات، دشواری نسبت دادن آنها به پدیدآورنده‌شان است. چنانچه هویت پدیدآورنده احراز نشود، هر اندازه ادله‌ها صحیحی و دقیق هم باشند، استنادپذیر نخواهند بود.
- ۲- با اینکه امکان شناسایی هرگونه تغییر در ادله‌ها وجود دارد، امام تغییر در آنها نیز بسیار آسان است.
- ۳- از بین بردن ادله‌ها بسیار آسان است. می‌توان با نصب یک برنامه نه چندان پیشرفته بر روی رایانه، تنظیم آن و زدن چند دکمه از صفحه کلید، تمامی ادله‌های مورد نظر را از بین برد.
- ۴- نقص سیستم یا رسانه ذخیره می‌تواند بر تمامیت ادله‌ها تاثیر گذارد. یکی از تفاوت‌های اصلی ادله‌های الکترونیکی با اسناد و مدارک فیزیکی در این است که به تنهایی در دنیای خارج وجود ندارد و همواره به یک سیستم یا رسانه وابسته‌اند. بنابراین هرگونه تغییر در وضعیت سیستم، بر وضعیت ادله‌ها تاثیر می‌گذارد.
- ۵- نقص برنامه‌های رایانه‌ای هم ایراد فوق را دامن می‌زند. هر ادله‌های که به یک سیستم رایانه‌ای وارد می‌شود، نوعی پردازش بر روی آن انجام می‌شود. حتی صرف نگهداری و ذخیره ادله‌ها در سیستم یا انتقال آنها بر روی یک رسانه نیز پردازش تلقی می‌شود. بنابراین حتی در ساده‌ترین حالت نیز ادله‌ها به یک یا چند برنامه، وابستگی کامل دارند. در نتیجه اگر آن برنامه‌ها دچار نقص باشند، بر خروجی ادله‌ها تاثیر مستقیم خواهند گذاشت.
- ۶- نسبت به اطلاعات فیزیکی، بیشتر در دسترس افراد غیرمجاز قرار دارند در حالی که دستیابی به یک سند یا مدرک فیزیکی برای افراد محدودی امکان‌پذیر است (گابتان، ۱۹۹۹: ۱۵۸)

۲- سیر سیاستگذاری ادله الکترونیکی

سرآغاز مشخصی برای پیدایش جرایم در فضای سایبر وجود ندارد. بسیاری اعتقاد دارند منشأ پیدایش جرایم فضای سایبر، به قضیه‌الدون رویس در سال ۱۹۶۳ میلادی در ایالات متحده آمریکا بر می‌گردد. اما آنچه مسلم است ایالات متحده آمریکا و کانادا از نخستین کشورهایی بودند که در اوایل دهه ۸۰ میلادی اقدام به تدوین قوانین و مقرراتی برای مبارزه و مقابله با جرم در فضای سایبر نمودند (گاوینگان، ۲۰۰۷: ۱۰۵). پس از آن در هفتمین کنگره پیشگیری از جرم و بسط عدالت کیفری سازمان ملل متحد که در سال

۱۹۸۵ میلادی برگزار شد، دبیر کل سازمان، برای نخستین بار گزارشی با عنوان پیشنهادهایی برای اقدام‌های هماهنگ بین‌المللی علیه شکل‌های به رسمیت شناخته شده جرایم ارائه کرد که در آن، درباره جرایم سایبری بحث مفصلی شد و کمیته پیشگیری از جرایم فضای سایبر و کنترل آن، عهده‌دار سازماندهی کوشش‌های بین‌المللی برای ارتقا و تعمیم چارچوبی جامع از خطوط راهنما و استانداردهایی شد تا به دولت‌های عضو در برخورد با جرایم سایبری کمک کند (لیند، ۱۹۹۷: ۹۷). طبق تعریف انجمن بین‌المللی جزا (AIDP)، جرایم سایبر به جرایمی گفته می‌شود که در محیطی غیرفیزیکی علیه ادله‌های حاصل از فناوری اطلاعات ارتکاب می‌یابد (سیگل، ۲۰۰۱: ۹۷). سازمان ملل متحد در تعریفی که از این نوع جرایم نموده، معتقد است جرایم فضای سایبر می‌تواند شامل فعالیت‌های مجرمانه‌ای باشند که ماهیتی سنتی دارند، اما با ابزار مدرنی همانند رایانه، شبکه و همه ابزارهای تشکیل‌دهنده فضای سایبر صورت می‌گیرد (کرو، ۲۰۰۷: ۸۶) در کشور ما نیز در تعاریفی که در قانون جرایم رایانه‌ای آمده است، این گونه جرایم به مواردی از قبیل: کلاهبرداری رایانه‌ای، جعل رایانه‌ای، جاسوسی رایانه‌ای، سابوتاژ رایانه‌ای (تغییر، محو، متوقف سازی، ملاحظه در خطوط ارتباطی و...) تخریب رایانه‌ای، دست‌یابی غیرمجاز، شنود غیر قانونی و... تقسیم شده است (باباغیبی ازغندی، ۱۳۹۲: ۱۴۹)

۲- ۱- ادله الکترونیکی در قوانین ایران

در ایران نیز تا آغاز دهه ۷۰ خورشیدی که استفاده از رایانه و فضای سایبر محدود بود، توجه چندانی به جرایم مرتبط با آن نشده بود. اگر جرمی هم در این خصوص واقع شده باشد، گزارشی از آن منتشر نشده است. از آغاز دهه ۸۰ خورشیدی بود که با پیشرفت روز افزون محبوبیت و کارایی فضای سایبر، جرایم مختلف دیگری چون: جعل اسکناس، اسناد و بلیط‌های شرکت اتوبوس‌رانی، گناهی‌نامه، کارت پایان خدمت، مدرک تحصیلی، چک، اشاعه فحشا و منکرات با انتشار عکس‌ها و تصاویر و مطالب خلاف عفت عمومی، ایجاد اختلاف میان اقشار جامعه از راه طرح مسائل قومی و نژادی، انتشار مطالب نژادپرستانه، انتشار اسناد و مسادل مجرمانه، اهانت به مقدسات مذهبی و دینی، اهانت و افترا نسبت به مقامات دولتی و اشخاص حقیقی و حقوقی، سرقت ادبی و... مطرح گردید (فضلی، ۱۳۸۵: ۸۲). از آن زمان تا کنون موارد متعددی از جرایم مختلف سایبر در حوزه‌های گوناگون در کشور ایران اتفاق افتاده است. بنابراین در راستای گسترش جرایم قوانین متعددی هم وضع شده است که در این بین ادله الکترونیکی به عنوان دلیل کشف حقیقت مورد تاکید قانونگذار بوده است که در جدول زیر به صورت خلاصه به آنها اشاره شده است:

جدول شماره ۱ - ادله‌های الکترونیکی در ایران

سال	سند یا پرونده	مفهوم
۱۳۸۲	قانون تجارت الکترونیکی	مفهوم ادله پیام در این قانون در ماده ۲ مورد تعریف قرار گرفته است. هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات، تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود.
۱۳۸۸	قانون جرایم رایانه‌ای	فصل دوم این قانون به جمع‌آوری ادله و همچنین مبحث چهارم این فصل به طور مشخص به تفتیش و توقیف و فصل چهارم به استنادپذیری ادله‌های الکترونیکی تصریح دارد.
۱۳۹۲	آیین دادرسی کیفری	بخش دهم این قانون از ماده ۶۶۴ تا ۶۸۷ به آیین دادرسی جرایم رایانه‌ای اختصاص یافته است. در این قانون نیز به تفتیش و توقیف و جمع‌آوری ادله‌های الکترونیکی تصریح شده است.
۱۳۹۳	آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی	این آیین‌نامه در خصوص ماده ۵۴ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ تصویب شده است که در آن جمع‌آوری، توقیف و تفتیش ادله‌های الکترونیکی تعریف و نحوه اقدام در این زمینه شفاف شده است.

۲-۲ - ادله الکترونیکی در قوانین چین

استفاده از ادله‌های الکترونیکی به‌عنوان ادله در دادرسی‌های کیفری در چین، دارای سابقه کوتاهی بوده است. بر اساس بعضی از نکات قابل توجه در زمان توسعه ادله‌های الکترونیکی در چین، در این بخش به تاریخچه حقوقی ادله‌های الکترونیکی در پرونده‌های کیفری در چین پرداخته شده است. به طور کلی، می‌توان توسعه ادله‌های الکترونیکی را به سه دوره تقسیم کرد. تا قبل از سال ۲۰۱۲، قانون آیین دادرسی جمهوری خلق چین، علی‌رغم ظهور ادله‌های الکترونیکی و تاثیر آنها بر مناسبات قضایی، آنها را به‌عنوان ادله در نظر نمی‌گرفت. از آنجا که این قانون از رویه‌های قضایی تبعیت نمی‌کند، محققان در اینکه ادله‌های الکترونیکی چه ویژگی‌هایی باید داشته باشند؟ و آیا باید تاثیر آنها در پرونده‌های کیفری را مورد پذیرش قرار داد؟ بحث و تبادل نظرهای جدی انجام داده‌اند. قانون آیین دادرسی کیفری جمهوری خلق چین در سال ۲۰۱۲ مورد تجدیدنظر قرار گرفت و در این اصلاحیه تاکید گردید که ادله‌های الکترونیکی، ادله فیزیکی و مبتنی بر مدرک و سند نیستند، بلکه نوع مستقلی از ادله‌های رایج، شناخته می‌شوند (بانگ و فینگ، ۲۰۲۱: ۳)

برای درک بهتر سیر سیاستگذاری حقوقی ادله‌های الکترونیکی در چین، برخی از نکات اساسی با جزئیات بیشتر در جدول شماره ۲ شرح ادله شده است.

جدول شماره ۲ - ادله‌های الکترونیکی در چین

سال	سند یا پرونده	مفهوم
۱۹۹۸	مقررات مربوط به مراحل رسیدگی به پرونده‌های کیفری	اصطلاح ادله‌های الکترونیکی اولین بار در یک سند رسمی قید گردید.
۲۰۰۵	مقررات شناسایی الکترونیکی ارگان‌های امنیت عمومی	داده‌های الکترونیکی به‌عنوان: ادله‌های ذخیره شده، پردازش شده و انتقال یافته به شکل دیجیتال تعریف شده است.
۲۰۱۲	قانون آیین دادرسی کیفری (اصلاحیه ۲۰۱۲)	داده‌های الکترونیکی به یک طبقه مستقل از ادله رایج تبدیل شدند
۲۰۱۶	مقررات مربوط به جمع‌آوری، نگهداری، بررسی و قضاوت ادله‌های الکترونیکی در رسیدگی‌های پرونده‌های کیفری	تعریف دقیق ادله‌های الکترونیکی: ادله‌هایی هستند که در جریان وقوع یک پرونده، ایجاد، ذخیره، پردازش و منتقل می‌شوند و می‌توانند واقعیت‌های پرونده را ثابت کنند. در عین حال شهادت شهود، اظهارت قربانی، اعتراف مظنون یا متهم در فرم دیجیتالی و سایر ادله ثبت شده، ادله‌های الکترونیکی نیستند.
۲۰۱۹	مقررات ادله‌های الکترونیکی به‌عنوان ادله برای مقامات امنیت عمومی در رسیدگی به پرونده‌های جنایی	روش‌های جمع‌آوری محدود شد و همچنین توجه ویژه‌ای به حمایت از حقوق حریم خصوصی اعمال گردید.

۳- بررسی تطبیقی مقررات ایران و چین در خصوص داده‌های الکترونیکی در امور کیفری

مقررات فعلی ایران و چین در خصوص داده‌های الکترونیکی به طور کلی شامل سه ویژگی، جمع‌آوری، توقیف و استنادپذیری است. به طور خلاصه مقررات اصلی حاکم در زمینه داده‌های الکترونیکی در ایران قوانین تجارت الکترونیکی مصوب سال ۱۳۸۲، قانون جرایم رایانه‌ای مصوب سال ۱۳۸۸ و آیین دادرسی کیفری مصوب ۱۳۹۲ و نیز آیین‌نامه جمع‌آوری و استنادپذیری داده الکترونیکی مصوب سال ۱۳۹۳ می‌باشد. مقررات شماره ۲۰۱۴، مقررات ۲۰۱۶ و قوانین ۲۰۱۹ مبنای اصلی داده الکترونیکی در چین می‌باشند. این مقررات، ضمن تبیین و روشن نمودن برخی از مفاهیم مهم مربوط به داده‌های الکترونیکی، مقررات جامع و منظمی را در مورد داده‌های الکترونیکی و کل روند رسیدگی قضایی بیان نموده‌اند. در بخش زیر به صورت جداگانه مرحله‌های جمع‌آوری، توقیف و استنادپذیری را در دو کشور ایران و چین به صورت تطبیقی مورد مطالعه قرار می‌دهیم.

۳-۱- جمع‌آوری و توقیف داده‌های الکترونیکی

جمع‌آوری و توقیف داده‌های الکترونیکی باید بر اساس قوانین و مقررات زیر در مورد، اشخاص جمع‌آوری و توقیف‌کننده، اشیاء جمع‌آوری و توقیف شده و روش‌های جمع‌آوری و توقیف مطابقت داشته باشد. در مواردی که این مقررات نقض شوند، داده‌های الکترونیکی در دادگاه قابل پذیرش نمی‌باشند. قانون جرایم رایانه‌ای مصوب سال ۱۳۸۸ تعریف دقیقی از جمع‌آوری داده الکترونیکی نکرده است ولی این نقص در بند د از ماده ۱ آیین‌نامه مربوط به ماده ۵۴ همین قانون مرتفع شده و این آیین‌نامه تعریفی از جمع‌آوری داده الکترونیکی به شرح زیر ارائه کرده است: فرایندی است که طی آن داده الکترونیکی به تنهایی یا به همراه سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده، نگهداری، حفظ فوری، تفتیش و توقیف و شنود می‌شوند. همچنین منظور از توقیف داده‌ها یا سامانه‌ها، حفاظت از آنهاست.

۳-۱-۱- متصدیان جمع‌آوری و توقیف داده الکترونیکی

قوانین و مقررات ایران در خصوص جمع‌آوری داده‌های الکترونیکی که در قانون جرایم رایانه‌ای و آیین‌نامه این قانون و همچنین قانون آیین دادرسی کیفری، این وظیفه را بر عهده ضابطان دادگستری محول کرده است. ماده ۶۷۰ آیین دادرسی کیفری مصوب ۱۳۹۲ تصریح دارد که ارائه‌دهندگان خدمات دسترسی موظف هستند بر اساس دستور قضایی داده‌های حفاظت شده را در اختیار ضابطان دادگستری قرار دهند. در حقیقت این قانون اشاره صریح دارد که جمع‌آوری داده الکترونیکی توسط ضابطان دادگستری انجام می‌گیرد. ماده ۶۶۹ قانون پیش گفته به ضابطان قضایی این اختیار را داده است در شرایط فوری نظیر خطر آسیب دیدن یا تغییر یا از بین رفتن داده‌ها، بتوانند دستور حفاظت را هم صادر نمایند. همچنین ماده ۶۷۹ این قانون اشاره دارد ضابطان با دستور مقام قضایی دامنه تفتیش و توقیف را به سامانه‌های دیگر گسترش می‌دهند و داده‌های مورد نظر را تفتیش یا توقیف می‌کنند. در همین راستا تبصره ۱ ماده ۱۱ و ماده ۱۳ و ماده ۲۰ و ماده ۴۳ آیین‌نامه جمع‌آوری و استنادپذیری داده الکترونیکی، از ضابطان یاد کرده است. آیین دادرسی کیفری مصوب ۱۳۹۲ در ماده ۲۹ ضابطان دادگستری را به عام و خاص تقسیم نموده است که در بند الف فرماندهان، افسران و درجه داران نیروی انتظامی را ضابطان معرفی کرده است. با توجه به تخصصی بودن این حوزه، در نیروی انتظامی جمهوری اسلامی ایران در سال ۱۳۹۱ پلیس فضای تولید و تبادل اطلاعات که به اختصار پلیس فتا نامیده می‌شود تاسیس گردید تا به جرایم در حوزه جرایم سایبری اعم از پیشگیری و تحقیقات مقدماتی بپردازد. پلیس فضای تولید و تبادل اطلاعات دارای معاونت‌های متعددی می‌باشد که یکی از معاونت‌هایی که در راستای داده الکترونیکی به صورت تخصصی فعالیت می‌نماید، معاونت فنی و داده دیجیتال می‌باشد. در مواردی که نیاز به جمع‌آوری و توقیف داده الکترونیکی باشد کارکنان و کارشناسان این معاونت با دستور مقام قضایی اقدام می‌نمایند. نکته حائز اهمیت در خصوص جمع‌آوری داده الکترونیکی اشاره آیین‌نامه جمع‌آوری و استنادپذیری داده الکترونیکی به اشخاص خبره می‌باشد. ماده ۱۳ آیین‌نامه اشعار می‌دارد: در موارد مقتضی، اجرای دستور حفاظت با نظارت ضابطان قضایی متخصص یا اشخاص خبره مورد وثوق به نمایندگی از طرف مرجع قضایی انجام می‌شود. در حقیقت قانون ایران در خصوص جمع‌آوری داده الکترونیکی، جایگاه اشخاص خبره را به رسمیت شناخته است. در مقررات کشور چین، در یک پرونده کیفری عادی، داده باید توسط محققان جمع‌آوری شود. با این حال، وقتی صحبت از داده‌های الکترونیکی به میان می‌آید، این فرایند ممکن است متفاوت باشد. در ابتدا، قانون شماره ۲۰۱۴ عنوان می‌کند، جمع‌آوری داده‌های الکترونیکی باید

توسط دو یا چند محقق با دانش فنی مربوط انجام گیرد. با این حال، ماده ۷ مقررات ۲۰۱۶، الزامی بودن داشتن دانش فنی مربوط را حذف کرده است. به عبارت دیگر، اینکه آیا این دو محقق دانش فنی لازم را در رابطه با جمع‌آوری ادله‌های الکترونیکی دارند؟، دیگر مورد توجه قرار نمی‌گیرد. با این وجود، طبق ماده ۶ قوانین ۲۰۱۹، جمع‌آوری ادله‌های الکترونیکی توسط دو یا چند محقق انجام می‌شود و در صورت لزوم، یک کارشناس متخصص می‌تواند به دستور محققان برای جمع‌آوری ادله‌های الکترونیکی به کارگیری شود. بنابراین کشور مقررات کشور چین در خصوص متصدیان جمع‌آوری ادله الکترونیکی، از طرفی مقامات امنیت عمومی را صالح به جمع‌آوری ادله الکترونیکی دانسته است و از سویی دیگر افراد متخصص حرفه‌ای را نیز تحت نظارت مقامات ذکر شده به رسمیت شناخته است. با ابتننا بر این وجه مشترک هر دو نظام حقوقی ایران و چین در خصوص جمع‌آوری کنندگان ادله الکترونیکی، صالح دانستن ضابطان دادگستری در ایران با محوریت معاونت فنی و ادله دیجیتال پلیس فتا و مقامات امنیت عمومی در چین و افراد خبره و متخصص در امر ادله الکترونیکی می‌باشد.

با وجود مقامات امنیت عمومی در چین برای جمع‌آوری ادله الکترونیکی، برجسته‌ترین مشکل رویه قضایی چین، کمبود بازرسان با دانش فنی در دستگاه‌های تحقیق‌کننده می‌باشد. علاوه بر این، موسسه‌های شخص ثالث، به طور فزاینده‌ای به عنوان افراد واجد شرایط برای جمع‌آوری ادله‌های الکترونیکی، اعلام موجودیت می‌کنند. برای مثال، سه شرکت غول پیکر اینترنت چین، علی بابا، تنسنت و باید و مجاز به جمع‌آوری ادله‌های الکترونیکی هستند. از آنجایی که آنها در این زمینه متخصص قلمداد می‌شوند، اجازه جمع‌آوری ادله الکترونیکی را از طرف محققان دارند. همچنین لازم به ذکر است که مطابق ماده ۵ قوانین ۲۰۱۹، ادله‌های الکترونیکی جمع‌آوری شده توسط آژانس دولتی دیگر، در جریان اجرای مقررات اداری، تا زمانی که این کار مطابق با مقررات اداری مربوط جمع‌آوری شده باشد، می‌تواند به عنوان ادله در پرونده‌های کیفری مورد استناد قرار گیرد. در مقابل مقررات کشور ایران، شرکت‌های خصوصی یا دولتی را صالح به اجرای دستورهای قضایی مبنی بر جمع‌آوری و توقیف ادله الکترونیکی به رسمیت نشناخته است. این مورد از وجوه تمایز این دو نظام حقوقی می‌باشد.

۲-۱-۳ روش‌های جمع‌آوری و توقیف ادله الکترونیکی

کلیه ادله‌های الکترونیکی مربوط به پرونده‌های کیفری باید به صورت جامع، علمی و بدون اعمال سلیقه شخصی و به موقع جمع‌آوری شوند. اولویت جمع‌آوری ادله‌های الکترونیکی، با محتوای اصلی می‌باشد. برابر ماده ۶۷۴ قانون آیین دادرسی کیفری مصوب سال ۱۳۹۲ تفتیش ادله‌ها یا سامانه‌های مخابراتی شامل اقدامات زیر می‌باشد: الف- دسترسی به تمام یا بخشی از سامانه‌های رایانه‌ای یا مخابراتی ب- دسترسی به حامل‌های ادله از قبیل دیسک‌ها یا لوح‌های فشرده یا کارت‌های حافظه ج- دستیابی به ادله‌های حذف یا رمزنگاری شده. بنابراین مقررات ایران در این ماده به سه روش اشاره دارد که با توجه به گستردگی ادله الکترونیکی، محدود بوده و روش‌های دیگر را شامل نمی‌شود. در مقابل مقررات کشور چین در ماده ۷ قوانین ۲۰۱۹، روش‌های جمع‌آوری را به پنج دسته خاص تقسیم می‌کند: الف) توقیف یا پلمپ کردن منبع ذخیره‌سازی اصلی، ب) به دست آوردن ادله‌های الکترونیکی از وبگاه‌ها، پ) به دست آوردن ادله‌های الکترونیکی به صورت برخط (آنلاین)، ت) انسداد ادله‌های الکترونیکی و ث) درخواست ادله‌های الکترونیکی از ارائه‌دهندگان خدمات دسترسی. در عمل، به طور معمول از چهار روش برای جمع‌آوری ادله‌های الکترونیکی استفاده می‌شود: جمع‌آوری از مسیر آنلاین، استخراج از محتوای اصلی، درخواست از شخص ثالث و تهیه توسط طرف‌های ذیربط. با توجه به مقررات نظام حقوقی ایران و رویه‌های جاری در محاکم و پلیس فتا می‌توان اینگونه استنباط نمود که به دست آوردن ادله الکترونیکی از وبگاه‌ها و نیز به صورت برخط در بند الف ماده ۶۷۴ به صورت ضمنی مورد اشاره قرار گرفته است. با ابتننا بر این هر دو نظام حقوقی روش‌های مشابهی را برای جمع‌آوری ادله الکترونیکی مورد استفاده قرار داده است، با این تفاوت که مقررات چین روش‌های جمع‌آوری را جزئی‌تر بیان نموده است. با وجود این رویه‌های عملی در مقررات ایران نیز جمع‌آوری به روش‌های دیگر را نیز در خود دارد. طبق قوانین ۲۰۱۹، محققان باید از مناسب‌ترین روش جمع‌آوری در عرف قضایی استفاده کنند تا فرایند جمع‌آوری، موثر و منطقی انجام پذیرد. علی‌رغم اینکه چین روش‌های کاربردی مفید جمع‌آوری ادله‌های الکترونیکی را گسترش داده است، با این وجود، پنج روش جمع‌آوری فعلی، دارای نواقص بالقوه می‌باشند. به عنوان مثال، هم ماده ۱۰ مقررات ۲۰۱۶ و هم ماده ۸ قوانین ۲۰۱۹ تجویز می‌کنند که در مواردی که به هر دلیل عینی جمع‌آوری یا گرفتن اطلاعات الکترونیکی انجام نشود، یا جمع‌آوری یا گرفتن ادله‌های الکترونیکی مطابق با سایر مقررات نامناسب باشد، ادله مربوط ممکن است با چاپ،

عکسبرداری یا ضبط فیلم جمع‌آوری و مورد استناد قرار گیرند. هدف این دو ماده به وضوح، تسهیل رسیدگی به پرونده‌ها و بهبود کارایی قضایی است. با این حال، این مواد چگونگی مخفی ماندن اطلاعات الکترونیکی را بیان نکرده‌اند، در نتیجه باعث اطلاع دادرسی در پرونده‌های کیفری می‌شود. علاوه بر این، به علت کمبود ادله‌های اصلی، برای وکیل مدافع مشکل است که اشکالات احتمالی ادله‌های الکترونیکی را شناسایی کند در نتیجه این موضوع، موقعیت آنها در دادگاه را با مشکل روبرو نموده و امکان نادیده گرفته شدن ادله مخفی متصور می‌باشد. این موضوع نیز حائز اهمیت است که زمان مصاحبه، تعدادی از قضات اظهار داشتند که آنها ترجیح می‌دهند ادله‌های الکترونیکی به صورت چاپی ارائه شوند زیرا ارزیابی ارزش اثباتی ادله‌های الکترونیکی ارسالی را برای آنها آسان می‌کند (فینگ، ۲۰۲۰: ۲۲).

۳-۳-۳- ملاحظات قانونی در جمع‌آوری و توقیف ادله الکترونیکی

با عنایت به اینکه استفاده از ادله الکترونیکی در دستگاه قضایی در راستای اثبات مجرمیت یا بی‌گناهی افراد مورد استناد قرار می‌گیرد، می‌بایست این ادله با اصول قانونی جمع‌آوری و توقیف شوند. هر دو نظام حقوقی ایران و چین در راستای جمع‌آوری ادله الکترونیکی توصیه‌هایی برای متصدیان جمع‌آوری و توقیف ارائه نموده است. در مقررات ایران ادله الکترونیکی مانند دیگر ادله اثبات دعوی می‌بایست با دستور مقام قضایی جمع‌آوری و توقیف شود، در حقیقت بدون دستور مقام قضایی جمع‌آوری و توقیف داده‌های الکترونیکی افراد جرم محسوب می‌گردد. ماده ۶۶۹ و ۶۷۱ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ به این موضوع تصریح دارد، فقط در شرایط فوری نظیر خطر آسیب دیدن یا تغییر یا از بین رفتن داده‌ها، ضابطان قضایی را مجاز دانسته است که بدون اخذ دستور قضایی اقدام به جمع‌آوری و حفاظت از ادله نمایند، البته این اقدام نیز حداکثر تا بیست و چهار ساعت به اطلاع مقام قضایی خواهد رسید. نکته مهم دیگر این است که جمع‌آوری، تفتیش و توقیف ادله الکترونیکی زمانی انجام می‌گیرد که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم صورت می‌گیرد. همچنین ماده ۲۸ آیین نامه جمع‌آوری و استنادپذیری ادله الکترونیکی اشعار می‌دارد: در مواردی که تفتیش یا توقیف طبق دستور قضایی بدون حضور متصرف قانونی یا شخصی که داده یا سامانه را تحت اختیار دارد، انجام پذیرد، مراتب پس از انجام فوراً به ذینفع ابلاغ خواهد شد. همچنین بند پ ماده ۶۷۶ آیین دادرسی کیفری رضایت متصرف قانونی را شرط توقیف سامانه‌های رایانه‌ای و مخابراتی دانسته است. در حقیقت قانونگذار ایران تأکید دارد که هرگونه جمع‌آوری، تفتیش و توقیف می‌بایست در حضور متصرف قانونی داده‌های الکترونیکی صورت گیرد تا حق و حقوقی از وی ضایع نگردد. در همین راستا ماده ۳۲ آیین نامه جمع‌آوری و استنادپذیری ادله الکترونیکی بیان می‌دارد رضایت متصرف قانونی سامانه باید کتبی و با امضای وی باشد. از سویی دیگر ماده ۳۱ همین آیین نامه اشخاصی را که داده‌ها یا سامانه‌های رایانه‌ای را یا مخابراتی را تحت کنترل و یا تصرف دارند را موظف نموده است با ضابطان دادگستری در خصوص تفتیش و توقیف همکاری نمایند ماده ۱ قوانین ۲۰۱۹ کشور چین، اشاره می‌نماید زمانی که ادله الکترونیکی به عنوان مدرک در محاکم کیفری قرار است مورد استناد قرار گیرند، دستگاه قضایی باید از کیفیت دستیابی به این ادله اطمینان حاصل نماید. همچنین در ماده ۲ این قانون به صورت کلی بیان شده است که مقامات امنیت عمومی باید هنگام رسیدگی به پرونده‌های کیفری، از رویه‌های قانونی پیروی کنند، در این راستا می‌بایست استانداردهای فنی مربوط لحاظ شود و ادله‌های الکترونیکی به طور جامع، عینی و به موقع جمع‌آوری شوند تا از صحت و درستی آنها اطمینان حاصل شود. بر اساس این می‌توان گفت که نظام حقوقی چین به صورت کلی مقامات جمع‌آوری ادله الکترونیکی را ملزم به رعایت قوانین جاری کشور چین و رعایت استانداردهای فنی نموده است. با نگاه به مقررات ایران و چین در خصوص رعایت حقوق شهروندی به نظر می‌رسد که مقررات ایران با حساسیت زیادی نسبت به جمع‌آوری، تفتیش و توقیف قانونگذاری نموده است و سعی داشته است با تحدید آزادی‌های ضابطان دادگستری در خصوص حریم خصوصی افراد مقابله نماید و این اجازه را ندهد که ضابطان دادگستری به بهانه اقدام‌های قضایی در خصوص ادله‌های الکترونیکی، حریم خصوصی افراد را نقض نمایند. این مورد می‌تواند نقطه قوت مقررات ایران نسبت به مقررات چین باشد. البته ماده ۶۷۸ قانون آیین دادرسی کیفری در موارد ضروری به ضابطان با دستور مقام قضایی اجازه داده است تا دامنه تفتیش و توقیف را به سامانه‌های دیگر هم گسترش دهند. ماده ۳۴ آیین نامه جمع‌آوری و استنادپذیری ادله الکترونیکی هم ضابطان را در حدود دستور قضایی مجاز به اقدام می‌داند مگر اینکه بیم امحا باشد که مجاز به اقدام هستند و باید حداکثر تا ۲۴ ساعت مراتب را

به مقام قضایی گزارش نمایند. یکی دیگر از نقاط قوت مقررات ایران ماده ۶۷۹ آیین دادرسی کیفری می باشد که در مقررات چین به چشم نمی خورد ماده مذکور بیان می دارد، توقیف داده ها یا سامانه های رایانه ای یا مخابراتی که موجب ایراد لطمه جانی یا خسارات مالی شدید به اشخاص یا اختلال در ارائه خدمات عمومی شود، ممنوع است مگر اینکه توقیف برای اجرای موضوع مهم نظیر حفظ امنیت کشور ضرورت داشته باشد. در این ماده نیز حقوق شهروندی تا حد امکان رعایت شده است تا به واسطه اقدام های ضابطان دادگستری ضررهای جانی و مالی به کسی وارد نگردد مگر در جایی که حقوق شهروندی و حفظ امنیت در تقابل هم باشند که قانونگذار حفظ امنیت را ارجح تشخیص داده است.

ماده ۶۷۲ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ ایران اشاره می کند که تفتیش و توقیف و جمع آوری داده ها یا سامانه های رایانه ای یا مخابراتی در حضور متصرفان قانونی یا اشخاصی که به نحوی آنها را تحت کنترل قانونی دارند، نظیر متصدیان سامانه ها انجام می شود. در صورت عدم حضور یا امتناع از حضور آنان چنانچه تفتیش یا توقیف ضرورت داشته باشد یا فوریت امر اقتضا کند، قاضی با ذکر دلایل دستور تفتیش و توقیف بدون حضور اشخاص مذکور را صادر می کند. بنابراین می بایست هر گونه اقدام روی ادله الکترونیکی با حضور متصرف قانونی و افراد واجد شرایط صورت گیرد و در صورت ضرورت بدون آنها نیز این اقدام صورت می پذیرد. در این خصوص ماده ۱۲ قوانین ۲۰۱۹ چین نیز تصریح دارد که رسانه های ذخیره اصلی باید با حضور شاهد و دارنده اصلی انجام شود. در مواردی که به دارنده اصلی یا شاهد در دسترس نبوده یا شناخته نشوند ماده ۱۳ این قانون اشاره دارد که جمع آوری و توقیف اجرا می شود و مراتب صورت جلسه شده و از روند کار فیلم برداری صورت گیرد. این مورد می تواند یکی از وجوه اشتراک هر دو نظام حقوقی ایران و چین باشد.

مورد دیگری که باید به آن اشاره کنیم این است که جمع آوری و توقیف شامل چه اطلاعاتی می شوند؟ ماده ۶۷۳ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ بیان می کند، دستور تفتیش و توقیف باید شامل اطلاعاتی از جمله اجرای دستور در محل یا خارج از آن، مشخصات مکان و محدوده تفتیش و توقیف، نوع و میزان داده های مورد نظر، نوع و تعداد سخت افزارها و نرم افزارها، نحوه دستیابی به داده های رمزنگاری یا حذف شده و زمان تقریبی انجام تفتیش و توقیف باشد که به اجرای صحیح آن کمک می کند. در حقیقت قانونگذار ایران در این ماده حدود و ثغور عملکرد ضابطان دادگستری را مشخص می کند و دستور باید شامل تمام جوانبی باشد که ماده اشاره نموده است، به نظر می رسد این ماده در راستای رعایت حقوق شهروندی می باشد تا ضابطان دادگستری نتوانند از حدود اختیارات قانونی فراتر روند. ماده ۲۴ آیین نامه جمع آوری و استنادپذیری ادله الکترونیکی نیز در همین راستا اشعار می دارد، ضابطان قضایی باید کلیه اطلاعاتی که ضرورت تفتیش و توقیف را ایجاد می نماید را در درخواست خود اعلام نمایند، همچنین موارد زیر را حسب مورد در درخواست تفتیش یا توقیف ذکر نمایند: الف - دلایل ضرورت تفتیش و توقیف. ب - حتی الامکان نوع و میزان داده ها و سخت افزارها ج - محل تفتیش یا توقیف د - دلایل لازم برای تصویربرداری و بررسی در خارج از محل ه - زمان تقریبی لازم برای تفتیش و توقیف. در ادامه مواد ۲۵، ۲۶ و ۲۷ این آیین نامه به مشخصات دستور قضایی نیز می پردازد و بیان می دارد، ماده ۲۵ - دستور تفتیش یا توقیف داده یا سامانه باید محل تفتیش یا توقیف تعیین و حتی الامکان در محل استقرار سامانه انجام پذیرد. ماده ۲۶ - مدت توقیف و فرصت اجرای تفتیش باید در دستور قضایی تصریح و کمترین فرصت ممکن منظور شود. در صورت نیاز به زمان بیشتر، به درخواست مجری تفتیش یا توقیف و ذکر علت آن، این مدت قابل تمدید می باشد. ماده ۲۷ - تفتیش و توقیف در مواردی که مستلزم ورود به منازل و اماکن خصوصی باشد، مطابق مقررات مندرج در آیین دادرسی کیفری خواهد بود.

۴-۱-۳ ملاحظات فنی جمع آوری و توقیف ادله الکترونیکی

از آنجایی که ادله الکترونیکی جز ابزارهای فناورانه می باشند و از وجهه تخصصی و فنی بالایی برخوردار هستند می بایست در جمع آوری و توقیف آنها، رعایت استانداردهای فنی و تخصصی الزامی می باشد. در همین راستا مقررات چینی در قوانین ۲۰۱۹ به صراحت رعایت استانداردهای فنی و تخصصی را در ماده ۲ بیان نموده است. شایان توجه است که ماده ۳۶ آیین نامه جمع آوری و استنادپذیری ادله الکترونیکی هم به علاوه بر داشتن شرایط لازم از قبیل تخصص و توانایی فنی و آموزش کافی، تجهیزات و وسایل لازم در اختیار را ضروری می داند. یکی از وجوه اشتراک دیگر هر دو نظام حقوقی ایران و چین تاکید روی داشتن تخصص متصدیان جمع آوری و توقیف می باشد. اما با دقت در مقررات چین به نظر می رسد نقطه قوت مقررات این کشور در مقابل مقررات ایران، نگاه تخصصی و فنی قانونگذار می باشد. قوانین ۲۰۱۹ موارد عدیده فنی و تخصصی را بیان کرده است که در

زیر به آنها اشاره نموده ایم. ماده ۱۱ این قانون اشاره دارد، وسیله ذخیره سازی توقیف شده باید با قرار دادن مهر و موم مطابق با الزامات زیر نگهداری شود: الف) تجهیزات الکترونیکی با قابلیت ذخیره سازی داده ها و اطلاعات و تجهیزات ذخیره ساز داخلی مانند هارد دیسک ها و کارت های حافظه را باید جداگانه نگهداری نمود. ب) در حین جمع آوری و توقیف می بایست از محل نگهداری و حالت و وضعیت ادله و سامانه های الکترونیکی مورد جمع آوری و توقیف عکس برداری و فیلم برداری نمود و این مستند سازی باید به وضوح مکان و نحوه قرار گیری را نشان دهد. پ) هنگامی که یک وسیله ذخیره ساز اصلی قابلیت ارتباط بی سیم داشته باشد مانند تلفن همراه باید سیگنال های ورودی و خروجی را مسدود نمود و برق را قطع نمود. با توجه به این ماده معلوم می گردد که قانونگذار چینی در صدد حفظ ادله الکترونیکی از طریق عکس برداری و فیلم برداری می باشد و در خصوص ابزارهای فناورانه ای چون گوشی تلفن همراه با خارج کردن گوشی از شبکه قصد دارد تا ادله از راه دور امحا یا تغییر نیابد. شایان توجه است که در رویه های پلیس فتا نیز این موضوع به صورت یک قانون نانوشته در حال اجرا می باشد، به این ترتیب که ضابطان به محض توقیف گوشی های همراه با قرار دادن ارتباط آن در حالت هواپیما کلیه ورودی ها و خروجی آن را مسدود می نمایند تا ادله الکترونیکی از طریق فضای سایبر و اینترنت امحا یا پاکسازی نگردد. ماده ۱۵ قوانین ۲۰۱۹ اشاره دارد که در جمع آوری و توقیف ادله الکترونیکی الف) باید مدیر اصلی ذخیره ساز اصلی و سیستم برنامه، معماری شبکه مشخص شود و اینکه آیا بیش از یک کاربر و مدیر وجود دارد یا خیر؟ هویت کاربران چیست؟ ب) نام کاربری و رمز عبور مدیریت ذخیره ساز اصلی و سیستم برنامه ها چیست؟ پ) آیا عملکرد خود تخریبی وجود دارد؟ آیا پشتیبان گیری از داده های ذخیره ساز اصلی صورت گرفته است؟ مکان پشتیبان گیری کجاست؟. با امعان نظر در این ماده مشخص می شود که قانونگذار چینی در صدد طرح ریزی برای یک جمع آوری و توقیف کارآمد است، چرا که ادله الکترونیک با توجه به ویژگی های خود در آن واحد قابل تحریف و حذف و تغییر است. ماده ۶۷۶ قانون آیین دادرسی کیفری شرایطی را برشمرده است که با وجود آنها سامانه های رایانه ای و مخابراتی که حاوی ادله الکترونیکی هستند توقیف می شود، آن شرایط به قرار زیر می باشند: الف) داده های ذخیره شده به سهولت در دسترس نباشند یا حجم زیادی داشته باشند. ب) تفتیش و تجزیه و تحلیل داده ها بدون سامانه سخت افزاری امکان پذیر نباشد. پ) متصرف قانونی سامانه رضایت داده باشد ت) تصویربرداری از داده ها به لحاظ فنی امکان پذیر نباشد. ث) تفتیش در محل باعث آسیب به داد ها شود. در مقابل ماده ۱۶ قوانین ۲۰۱۹ شرایطی را بیان می کند که نمی توان در آن شرایط سامانه ذخیره سازی اصلی که حاوی ادله الکترونیکی می باشد را توقیف کرد، بلکه می بایست سر صحنه ادله را دریافت نمود، آن شرایط به شرح زیر می باشند: الف) محیطی که ذخیره ساز اصلی در آن قرار دارد، مناسب مهر و موم کردن نیست. ب) داده های حافظه رایانه، داده های انتقال شبکه یا سایر داده های الکترونیکی که در یک حافظه ذخیره ساز تجمع نمی شوند. پ) رسیدگی به پرونده فوریت دارد و عدم دریافت فوری ادله الکترونیکی ممکن است منجر به از بین رفتن ادله الکترونیکی شود که عواقب جدی را با خود به همراه داشته باشد. ت) خاموش کردن تجهیزات الکترونیکی ممکن است باعث توقف عملکرد یک سیستم اطلاعات مهم شود. ث) غربالگری محیط ذخیره ساز مشکوک با توقیف داده های الکترونیکی در صحنه ضرورت داشته باشد. ج) زمانی که سیستم اطلاعات رایانه یا برنامه خاموش شود و دریافت ادله بدون رمز عبور غیر ممکن شود. این موارد که بیان گردید، اموری فنی و تخصصی می باشد که متصدیان مجرب جمع آوری و توقیف باید ضرورت آن را در صحنه اقدام تشخیص دهند و با صورتمجلس برای درج در پرونده نگهداری نمایند.

ماده ۱۷ این قانون نیز شرایطی برای عملیاتی نمودن ماده قبل بیان نموده است، به عبارت دیگر موارد زیر می بایست زمانی که ادله الکترونیکی در صحنه دریافت و توقیف می شوند باید رعایت گردد: الف) در اسرع وقت فرد متهم باید از تجهیزات الکترونیکی که ادله الکترونیکی در آن ذخیره شده است را دور گردد. ب) اگر آسیب جدی به داده های الکترونیکی وارد نمی شود، سیستم نباید خاموش گردد. پ) اگر امکان کنترل سیستم رایانه ای از راه دور متصور است، اقداماتی مانند ارسال سیگنال پارازیت، مسدود کردن سیگنال و قطع شبکه باید صورت گیرد. ج) حفاظت از منبع تغذیه برق سیستم باید در اولویت باشد. در راستای جمع آوری و توقیف فنی و تخصصی ادله الکترونیکی مقررات ایران در ماده ۳۷ آیین نامه جمع آوری و استنادپذیری ادله الکترونیکی موارد زیر را بیان کرده است: الف) شیوه اقدام نباید موجب تغییر، امحا یا جابجایی داده های مورد نظر در سامانه رایانه ای باشد. ب) تفتیش صرفاً در محدوده دستور قضایی و داده های مرتبط با جرم موضوع دستور، انجام می پذیرد. پ) کلیه فرایندهای انجام شده بر روی داده های

مورد تفتیش یا توقیف با استفاده از روش های قابل تشخیص، ثبت و محافظت شود. همچنین ماده ۳۸ آیین نامه پیش گفته بیان می دارد: توقیف داده ها از طریق چاپ داده ها، غیر قابل دسترس کردن داده ها به روش هایی از قبیل تغییر گذر واژه ها یا رمزنگاری و ضبط حامل های داده صورت می گیرد.

از بررسی مقررات فوق، می توان دریافت که اقدام های فنی در مورد موضوع های آیین نامه ای برای اطمینان از صحت و اصالت ادله های الکترونیکی، مورد تاکید هستند. با این حال، این مقررات این موضوع را نادیده می گیرند که توقیف ادله های الکترونیکی بیشتر یک موضوع آیین نامه ای (رویه ای) است. در چین، محدودیت توقیف به اندازه کافی برای اطمینان از همخوانی ادله های الکترونیکی ایجاد نشده است، به این معنی که ادله های الکترونیکی می توانند بین زمان ایجاد و ارائه آن در دادگاه به عنوان مدرک، تغییر، دستکاری یا آسیب ببینند. در نتیجه این موضوع، دادگاه این امکان را دارد که اصالت ادله های الکترونیکی برای استفاده در دفاع، مورد خدشه قرار دهد، در عین حال، عدم قابل استناد بودن ادله های الکترونیکی را نیز تشدید می کند. (ماسون و سینگ، ۲۰۱۷: ۱۹۶) علاوه بر این، از آنجا که ظرفیت و منابع در نقاط مختلف چین متفاوت است، برخی از مناطق چین حتی اتاق های خاصی را برای نگهداری ادله برای اطمینان از یکپارچگی ادله های الکترونیکی تعیین نکرده اند. بنابراین، قبل از استفاده از فناوری های خاص در روند توقیف ادله های الکترونیکی، نیازهای عملی و مسائل رویه ای مورد توجه قرار می گیرد.

۳-۳ - استنادپذیری ادله های الکترونیکی

از آنجایی که ادله های الکترونیکی غیر ملموس هستند، می توانند به راحتی تغییر کنند- حتی با عمل ساده روشن یا خاموش کردن کامپیوتر. استنادپذیری ادله های الکترونیکی همیشه یک مسئله اصلی در دادگاه های کیفری بوده است. آنچه در بحث استنادپذیری ادله الکترونیکی حائز اهمیت است، این است که این ادله در طبقه بندی ادله سنتی جای نمی گیرند. در حقوق کیفری ایران با اینکه قانون جرایم رایانه ای مصوب ۱۳۸۸ به طور خاص در بخش دوم تحت عنوان آیین دادرسی فصل دوم را به جمع آوری ادله الکترونیکی اختصاص داده است. امام بحثی از ارزش اثباتی این ادله به میان نیاورده است. با این حال یکی از نوآوری هایی که قانون تجارت الکترونیکی در سال ۱۳۸۲ در نظام حقوقی ایران به وجود آورد اعتبار بخشیدن به دلایل الکترونیکی در مراجع قضایی می باشد (موذن زادگان و شایگان، ۱۳۸۸: ۸۳). در خصوص ارزش اثباتی دلایل الکترونیکی در حقوق ایران قانون تجارت الکترونیکی در ماده ۱۲ بر اصل لزوم پذیرش دلایل الکترونیکی از سوی محاکم و ادارت تصریح کرده و مقرر می دارد: اسناد و ادله اثبات دعوی ممکن است به صورت ادله پیام بوده و هیچ محکمه یا اداره دولتی نمی تواند بر اساس قواعد ادله موجود، ارزش اثباتی ادله پیام را صرفاً به دلیل شکل و قالب آن رد کند. شایان توجه است که هر نوع ادله پیامی نمی تواند معتبر باشد بلکه مطابق ماده ۱۴ قانون تجارت الکترونیک ادله پیام هایی که به طریق مطمئن ایجاد و نگهداری شده اند در حکم اسناد معتبر و قابل استناد در مراجع قضایی و حقوقی می باشند.

در کشور چین اصالت و یکپارچگی ادله های الکترونیکی در سه مقررات ذکر شده در بالا مورد تاکید قرار گرفته است، در حالی که مواد مربوط به تایید اعتبار ادله های الکترونیکی کم می باشد و اصولی در شماره های ۲۰۱۴ و مقررات ۲۰۱۶ است. در مقایسه شماره ۲۰۱۴ و مقررات ۲۰۱۶ و قوانین ۲۰۱۹ روش های فنی اعمال شده برای اطمینان از صحت ادله های الکترونیکی است.

در شماره ۲۰۱۴، ماده ۱۷ فقط به طور خلاصه به این موضوع می پردازد و از نهاد امنیت عمومی می خواهد بدون ذکر جزئیات روش های خاص تایید صحت، اطلاعات مربوط به آمار ادله ها و اصالت آنها را ارائه نماید. ۲۹ مقررات ۲۰۱۶ شامل مواد پیچیده ای در مورد استنادپذیری ادله های الکترونیکی است. طبق ماده ۲۵ مقررات ۲۰۱۶، روش های تایید آدرس IP مربوط، سوابق فعالیت شبکه، انتساب پایانه های اینترنتی، شهادت شهود مربوط و همچنین اقرار و استدلال های متهم می توانند برای قضاوت جامع در مورد یکسان بودن هویت آنلاین و هویت واقعی متهم کمک کنند. با این وجود، روش های استنادپذیری ادله های الکترونیکی در مقررات ۲۰۱۶، به ویژه به روش های اعمال شده بر ادله متعارف شباهت دارد، به طوری که ویژگی های منحصر به فرد داده های الکترونیکی نادیده گرفته می شود. به عنوان مثال، از نظر یکسان بودن، مقررات ۲۰۱۶ بر این موضوع تاکید می کند که آیا هویت آنلاین و هویت واقعی متهم یکسان است؟ در حالی که دشواری هایی را که هنگام قضاوت درباره شخص واقعی پنهان در پشت هویت آنلاین وجود دارد، نادیده می گیرد. علاوه

بر این، برای اینکه انواع ادله معتبر باشند، باید ثابت شود که ادله همان چیزی است که ادعا می‌کنند. با این حال مواد مقررات ۲۰۱۶ نمی‌توانند به این سوال درباره ادله‌های الکترونیکی پاسخگو باشد.

فصل ۳ قوانین ۲۰۱۹، به بررسی و بازخوانی تحقیقات درباره ادله‌های الکترونیکی متمرکز شده است. مطابق ماده ۵۰ قوانین ۲۰۱۹، در صورت لزوم، با تایید فردی که مسئول امنیت عمومی در سطح شهرستان یا بالاتر از آن است، می‌توان یک تحقیق در مورد ادله‌های الکترونیکی انجام داد. اقدامات مکرر تحقیقاتی درباره ادله‌های الکترونیکی، معمولاً برای تایید برخی ناهنجاری‌ها یا تغییر در ادله‌های الکترونیکی انجام می‌شود، بررسی اینکه آیا برخی اقدامات عملیاتی روی ادله‌های الکترونیکی می‌توانند در مدت زمان مشخصی به اتمام برسند، بررسی اینکه آیا از نرم‌افزار یا سخت‌افزار خاصی می‌توان برای انجام عملی خاص استفاده کرد؟ یا عواقب خاص و تعیین اینکه آیا یک برنامه خاص سیستم اطلاعات رایانه‌ای می‌تواند ادله‌های الکترونیکی خاص را اصلاح کند؟ ۳۰ در همان زمان، اقدامات مجدد بررسی ادله‌های الکترونیکی باید شرایط زیر را داشته باشند: ۱- از اقدام‌های فنی برای محافظت از یکپارچگی ادله‌ها در یک منبع ذخیره‌سازی اصلی استفاده می‌شود. ۲- در صورت وجود شرایط، باز آزمایشی تحقیقاتی ادله‌های الکترونیکی باید دو یا بیشتر انجام شود. ۳- تجهیزات الکترونیکی، محیط شبکه و موارد مشابهی که در بازجویی‌های تحقیقاتی استفاده می‌شود باید با صحنه جرم سازگار باشد. در صورت لزوم، می‌توان از روش‌های فنی مربوط برای شبیه‌سازی یا انجام آزمایش کنترل شده در محیط مناسب استفاده کرد. ۴- رفتاری که ممکن است اطلاعات شهروندان را افشا کند یا بر عملکرد طبیعی سیستم‌های اطلاعات رایانه‌ای در محیط‌های غیرآزمایشی تاثیر بگذارد، ممنوع است.

نتیجه‌گیری

آنچه تلاش شد در این نوشتار تبیین گردد، مطالعه تطبیقی ارزیابی ادله الکترونیکی در نظام حقوقی ایران و چین به منظور درک بهتر نقاط قوت و ضعف نظام‌های حقوقی برای رفع خلاءهای موجود در قوانین کشور ایران بر اساس تجارب کشور چین است. مقامات چینی و ایرانی تلاش زیادی برای افزایش مقررات مربوط به ادله‌های الکترونیکی در دهه‌های گذشته انجام داده‌اند. با این وصف، هنوز جای توسعه بیشتر مقررات مربوط وجود دارد. با نگاهی هر دو نظام مورد مطالعه می‌توان نتیجه گرفت که نظام حقوقی ایران در زمینه رعایت حقوق متهمان و شهروندان پیشروتر از نظام حقوقی چین در زمینه جمع‌آوری و توقیف و استنادپذیری می‌باشد، در این راستا هر اقدامی را منوط به کسب اجازه از مقام قضایی نموده و حدود اختیارات ضابطان قضایی را تشخیص و تحدید نموده است. از نقاط قوت دیگر نظام حقوقی ایران می‌توان به انسجام قوانین جرایم رایانه‌ای اعم از قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و آیین دادرسی کیفری این جرایم و آیین‌نامه جمع‌آوری ادله الکترونیکی و استنادپذیری می‌باشد. در مقابل می‌توان بیان نمود که از نقاط ضعف مقررات چینی، نگاه کلی از منظر قانونی به موضوع می‌باشد و حدود اختیارات مقام‌های امنیت عمومی رسیدگی‌کننده با قوانین کلی گسترده بوده و امکان نقض حقوق شهروندی متصور می‌باشد. همچنین از آنجایی که ضریب نفوذ اینترنت در چین بیشتر از ایران بوده است ولی قوانین پراکنده‌ای در این زمینه وضع شده است. از نقاط قوت نظام حقوقی چین در زمینه موضوع مورد مطالعه می‌توان به نگاه تخصصی به جمع‌آوری و توقیف ادله الکترونیکی می‌باشد. در حقیقت قانونگذار چینی با رویکرد فنی مواردی که امکان دارد در آن شرایط بهترین عملکرد حاصل گردد را بیان نموده و شرایطی که در آن امکان محو، تغییر و امحا ادله الکترونیکی وجود دارد را بیان نموده و راهکارهای تخصصی به محققان و افراد خبره خود نشان داده است. در مقابل این ضعف در قوانین ایران مشهود است، درست است که قانونگذار ایران موارد فنی را به صورت کلی بیان نموده است، ولی در عرصه عمل معاونت فنی و ادله دیجیتال پلیس فتا به عنوان ضابط به صورت فنی این موارد را رعایت می‌نماید. از دیگر نقاط قوت مقررات چینی استفاده از افراد خبره و متخصص در زمینه جمع‌آوری و توقیف و استنادپذیری می‌باشد تا جایی که از شرکت‌های خصوصی نیز در این زمینه استفاده می‌نماید که به نمایندگی امور مربوط به پرونده‌های کیفری با ادله الکترونیکی را انجام می‌دهند. این موضوع در قوانین ایران دیده نشده است ولی شاید بتوان با عموماً قانون آیین دادرسی کیفری در بخش ارجاع امر به کارشناس این خلا را جبران نمود. در حقیقت مقام قضایی می‌تواند با ارجاع امر به کارشناس با شرایطی که در قانون آیین دادرسی کیفری دیده شده است، ادله الکترونیکی را جمع‌آوری و توقیف و مورد استناد

قرار دهد. از مشترکات هر دو نظام حقوقی می‌توان به متصدیان جمع‌آوری و توقیف اشاره نمود که در هر دو نظام این اقدام توسط نیروی پلیس صورت می‌پذیرد، در کشور چین مقامات امنیت عمومی و محققان پلیس با کمک افراد فنی و متخصص و در ایران ضابطان دادگستری که به طور خاص کارکنان پلیس فتا و معاونت فنی و ادله دیجیتال این پلیس که از میان افراد تحصیلکرده در زمینه رایانه و ابزارهای فناورانه انتخاب می‌شوند و افراد متخصصی می‌باشند، صورت می‌پذیرد. بر همین اساس می‌توان به مواردی برای تحقیقات آینده، محققان و پژوهشگران اشاره نمود. تقویت مقررات در آینده شامل ایده حمایت از حقوق و تعامل بین فن‌آوری‌های جدید و نظریه ادله است. از یک طرف، تقویت ایده حمایت از حقوق این افراد در برابر تحقیقات غیرقانونی، به ویژه حق آنها برای دانستن، حفظ حریم خصوصی و حقوق مالکیت ضروری است. اهمیت پیشگیری از افشا اطلاعات در روند جمع‌آوری ادله‌های الکترونیکی باید در مقررات در نظر گرفته شود. علاوه بر این، از منظر قانونگذار، ادله‌های الکترونیکی به دست آمده غیرقانونی، بلافاصله باید در محدوده استثنای ادله به دست آمده غیرقانونی قرار گیرند. در واقع استنادپذیری ادله الکترونیکی که از طریق نامشروع کسب و جمع‌آوری شده‌اند می‌تواند به عنوان ضمانت اجرای حداقلی در راستای صیانت از حقوق افراد در برابر اقدامات غیرقانونی کنشگران نظام عدالت کیفری در حوزه مبارزه با جرائم الکترونیکی مورد توجه باشد مگر در موارد مهم و دارای ابعاد امنیتی که ادله تحصیلی مرتبط با مصالح عمومی مردم است. فقط با انجام این مراحل می‌توان از حقوق محرمانه مظنون در طی فرایند جمع‌آوری اطلاعات الکترونیکی کاملاً محافظت کرد. از سوی دیگر، توسعه فن‌آوری‌های جدید نظریه‌ها و قوانین ادله موجود را به چالش کشیده است. علاوه بر فن‌آوری بلاکچین که می‌تواند به عنوان ابزاری برای استنادپذیری ادله‌های الکترونیکی با توجه به چندین موضوع در مورد رسیدگی به پرونده‌ها توسط دادگاه‌های اینترنتی مورد استفاده قرار گیرد. با این حال در زمینه جمع‌آوری، استنادپذیری و توقیف ادله‌های الکترونیکی نظام حقوقی ایران با چالش‌هایی روبرو است. در راستای رفع این چالش‌ها ارتقا سطح دانش فنی در شیوه‌های جمع‌آوری، توقیف و استنادپذیری در مراجع قضایی و ضابطان دادگستری به ویژه پلیس فضای تولید و تبادل اطلاعات (فتا) از ضروریات می‌باشد. از طرفی با توجه به گسترش و پیچیده شدن فضای سایبر و مهاجرت خیلی از جرایم به فضای سایبر، نیازمند بروزرسانی و تجدیدنظر در قانون جرایم رایانه‌ای با توجه به مقتضیات روز فن‌آوری می‌باشیم.

منابع:

- امامی، حسن (۱۳۷۰) حقوق مدنی، تهران، انتشارات اسلامی.
- باباغبی ازغندی، علیرضا (۱۳۹۲) الگوی نوین برای پیشگیری از جرایم فضای سایبر، فصلنامه مطالعات پیشگیری از جرم، سال ۸، شماره ۲۶، بهار، ۱۴۳-۱۶۸.
- پچی، آئورلیو (۱۳۸۴). جهان در آستانه قرن بیست و یکم، ترجمه عزت الله فولادوند، چاپ اول، تهران، انتشارات انقلاب.
- شمس، عبدالله (۱۳۹۰) آیین دادرسی مدنی، جلد اول، تهران، انتشارات دراک.
- شهبازی نیا، مرتضی؛ عبداللهی، محبوبه (۱۳۸۹) دلیل الکترونیک در نظام ادله اثبات دعوا، فصلنامه حقوق، دانشکده حقوق و علوم سیاسی تهران، شماره چهارم، دوره چهل، ۲۰۵-۱۹۳.
- عابدینی، زین العابدین (۱۳۸۸) جرم در فضای سایبر و ضرورت مطالعات آینده پژوهی، نشریه کارآگاه، شماره نهم، ۱۴۴-۱۵۶.
- فضلی، مهدی (۱۳۸۵) بررسی مسئولیت کیفری ارائه‌دهندگان خدمات اینترنتی، پایان نامه دوره کارشناسی ارشد حقوق جزا و جرم شناسی، دانشگاه تهران، پردیس قم.
- مدنی، سید جلال الدین (۱۳۸۵) آیین دادرسی مدنی، جلد دوم، ویرایش سوم، تهران، انتشارات گنج دانش.
- معین، محمد (۱۳۸۰) فرهنگ لغت فارسی، جلد اول، تهران، انتشارات سروش.

مودن زادگان، حسنعلی، شایگان، محمدرسول (۱۳۸۸) استنادپذیری و تحصیل ادله الکترونیکی در حقوق کیفری ایران، فصلنامه دیدگاه‌های حقوقی دانشکده علوم قضایی و خدمات اداری، شماره ۴۸، زمستان، صص ۷۷-۱۰۲

Crowe, T.(2001) crime prevention through environmental design, butterworth-heinmann, oxford, great britain

Galina Borisevich et al., 'A Comparative Review of Cybercrime Law and Digital Forensics in Russia, the United States and Under the Convention on Cybercrime of the Council of Europe' (2012) 39 N. Ky. L. Rev. 267..

Gavigan, a (2007) digital crime, Ankara publisher, turkry

Haisong Yu, 'Criminal Electronic Data: Regulatory Approaches and Key Issues' (2019) 1 Global Law Review 39.

Hao Cui, 'Legal Thinking of Electronic Evidence in Cybercrime' (2007) 2 Criminal Research 51

Jiao Feng, 'On the Custody of Internet Evidence' (2018) 1 Nanjing University Law Review 298

Jiao Feng, 'The Production of Internet Evidence' (2020) 4 Journal of Harbin Institute of Technology (Social Sciences Edition) 22.

m. gabtan, alan(1999). Electronic evidence. Carswell.

Minyuan Wang, 'A Study on the Judicial Interpretations of Criminal Procedure Law after the Amending in 2012' (2015) 1 Journal of National Prosecutors College 131.

Rong Hu, 'Application of the Location Service and Its Legislation in the Criminal Investigation' (2020) 4 Study & Exploration 60.

Rong-Shu-Xia Computer Ltd. v China Society Publisher, by Minyan Wang (2007) 4 Digital Evidence and Electronic Signature Law Review 95

Seigel, B. (2001), crime prevention, oxford of criminology, great britain,

Stephen Mason & Daniel Seng, editors, 'Electronic Evidence (Fourth Edition)' (2017) Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London 196.

Tonghui Zhu & Yuqing Wang, 'Due Process Regulation of Electronic Data Collection' (2020) 1 Journal of Soochow University (Law Edition) 130

Weiqiu Long & Wei Pei, 'Concept and Authentication of Digital Evidence' (2016) 2 Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition) 40.

Wenjiang Hao, 'A Probe on the Independent Status of Electronic Evidence in Procedure Law' (2007) 3 Journal of Political Science and Law 40

Xingdong fang & shuai chen, twenty five years of internet in china(2019) modern communication, journal of communication university of china.

Yongsheng Chen, 'Construction of the System of Search and Seizure of Electronic Communication Data' (2019) 1 Global Law Review 19.

Yongsheng Chen, 'The Challenges of the Cybercrime to Criminal Procedure and its Systematic Response' (2014) 3 Science of Law (Journal of Northwest University of the Political Science and Law) 149.