Pontificia Universidad Católica Madre Y Maestra

Decanato de Postgrado

Área de Ciencias Sociales y Humanidades y Artes

Trabajo de investigación final para optar por el título de
Magíster en Ciencias Penales

"El ciberdelito de clonación de tarjetas bancarias en la República Dominicana"

Sustentante:
Eugenia del Pilar Polanco Disla
1014-1918

Asesora de contenido:
Esther Elisa Agelán Casasnovas

Asesora metodológica:
Gisell López Baldera

Santiago de los Caballeros
República Dominicana
Julio, 2022

Pontificia Universidad Católica Madre Y Maestra

Vicerrectoría Académica

Área de Ciencias Sociales y Humanidades y Artes

Decanato de Postgrado

Formulario de Cesión Derechos de Autor al Repositorio Institucional Investigare

Este documento establece los derechos que usted otorga relacionados a la publicación de su trabajo académico, mediante su inclusión en el *repositorio del sistema de biblioteca de esta institución (PUCMM).* No habrá ningún pago para usted por esta publicación y por el otorgamiento de los derechos de esta.

Usted confirma que

> Este trabajo académico es original propio que no infringe los derechos de autor de otros; en caso de no ser un trabajo completamente original, declara que tiene los permisos necesarios por escrito de este otorgamiento por parte de demás autores.
> El contenido de este trabajo académico no contiene ningún material que sea difamatorio, viole los derechos de privacidad, o revele la información confidencial.
> Este trabajo académico no se ha publicado en parte o en su totalidad, y usted no publicara este trabajo académico en ningún otro lugar sin el consentimiento del repositorio institucional.
> Este trabajo académico se ha conducido respetando los principios éticos establecidos por la institución.

Usted otorga los derechos de autor de este trabajo académico al repositorio institucional (PUCMM), a nivel mundial, de manera perpetua y sin pagos; y en la medida requerida por los términos de este acuerdo. Conservara en todo momento el derecho a ser reconocido como el autor del trabajo académico. Además, acepta que el repositorio de la PUCMM tiene el derecho de tratar este trabajo académico como se considere oportuno (por ejemplo, derecho a imprimir, publicar, comercializar, comunicar y distribuir en todos los medios, editar la forma del trabajo, registrar los derechos de autor, cumplir con la política editorial establecida por el repositorio, entre otros).

He leído, entiendo y acepto los términos anteriores.

Nombre del Programa: Maestría en Ciencias Penales.

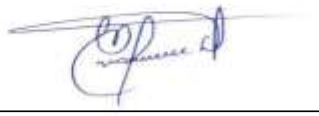
Título del Trabajo: El ciberdelito de clonación de tarjetas bancarias en la Republica Dominicana.

Nombre (s) y Apellidos: Eugenia del Pilar Polanco Disla.

Matrícula: 1014-1918.

Cedula de Identidad y Electoral: 095-0019985-7.

Fecha (día, mes, año): 15/07/2022.

Firma  _____

“El ciberdelito de clonación de tarjetas bancarias en la República Dominicana”

DEDICATORIA

A todos mis seres queridos, por el apoyo incondicional que me brindan siempre.

Eugenia del Pilar Polanco Disla

AGRADECIMIENTOS

A Dios todopoderoso, con él todo sin él nada.

A los profesores y asesores, por ser excelentes formadores y haber contribuido con mi formación durante estos últimos años.

A todo aquel familiar, amigo, compañero, que de una forma u otra me tendió su mano y me ayudó a concluir este proyecto.

Eugenia del Pilar Polanco Disla

Tabla de Contenido

Introducción

Resulta muy común que en las sociedades modernas prevalezca el uso de tecnologías en cualquier esfera de la vida. Por tal razón, en los últimos años, tanto en el plano nacional como internacional se han duplicado los hechos en los que, valiéndose de medios telemáticos o informáticos, se adquieren de forma fraudulenta datos personales de usuarios con productos bancarios que luego son usados para cometer ciertas actividades ilícitas, haciéndole cargos por consumo o defraudando las cuentas bancarias a los titulares de estas. Este es el denominado delito de clonación de tarjeta, considerado uno de los delitos o crímenes con mayor incidencia en la República Dominicana.

Es importante destacar que el ciberdelito de clonación de tarjeta es un delito que requiere un trato especial porque tiene que ver directamente con el robo de nuestros datos personales y financieros con fines fraudulentos, y que vulneran tanto nuestro derecho a la intimidad, a la protección de nuestros datos confidenciales como también a nuestro patrimonio económico.

Por otra parte, desde finales del año 2019 se ha vivido una situación que nadie se esperaba y es lo que ha sido denominada pandemia COVID-19. Esta a su vez trajo consigo una serie de cambios, entre ellas el confinamiento en nuestros hogares convirtiéndose por tanto, los medios electrónicos y el internet, en nuestros mejores aliados. Sin embargo, así cómo las personas se han tenido que volver más diestras en el área de la tecnología, de igual forma lo han hecho los ciberdelincuentes quienes han aprovechado la virtualidad y la misma pandemia para realizar cada vez mas fechorías.

Afortunadamente, en los tiempos actuales hay un sin número de herramientas que permiten divisar si algun virus o programa intenta robar información personal así como tambien, existen leyes y organismos que buscan proteger al individuo víctima de algun delito cometido a traves del ciberespacio e investigar y sancionar al que comete tales acciones.

Este estudio ha planteado como objetivo general analizar el desarrollo del ciberdelito de Clonación de Tarjeta durante los años 2018 a 2021 en Santiago de los

Caballeros; al mismo tiempo, los objetivos específicos son los siguientes: analizar las técnicas fraudulentas utilizadas por los ciberdelincuentes para cometer sus infracciones, evaluar el impacto del ciberataque de clonación de tarjeta durante la pandemia COVID_19 y, finalmente, determinar las acciones judiciales que se pueden realizar a fin de prevenir y combatir este tipo de crímenes-delitos y cómo puede resarcirse el daño causado.

Esta investigación se ha estructurado en tres capítulos divididos a su vez en subtemas. Cada uno contiene el desarrollo de los temas que sirven de soporte en cuanto a los aspectos teóricos sobre los que se basa el presente trabajo. A continuación, se hará un breve bosquejo del contenido general de este trabajo investigativo.

En el primer capítulo se desarrolla todo lo concerniente a la base conceptual y normativa en materia de ciberdelitos o delitos informáticos en la República Dominicana en sentido amplio. A su vez, esta sección está dividida en cuatro temas; cada tema trata de darnos una aproximación teórica sobre el fenómeno de los ciberdelitos o delitos informáticos: origen, evolución, definición, características y clasificación. En el último tema se despliega el marco normativo y regulatorio de los ciberdelitos y la legislación aplicable tanto en el ámbito nacional como en el internacional.

En el segundo capítulo se detalla de manera específica todo lo relacionado con el ciberdelito de clonación de tarjetas. Este apartado está dividido en cinco temas; se comienza explicando qué es una tarjeta bancaria para desde allí poder expresar qué es clonación de tarjeta y cómo se tipifica y sanciona en la República Dominicana. Asimismo, se detallan cuáles son los diferentes métodos utilizados por los ciberdelincuentes para clonar tarjetas, cuáles derechos y libertades se afectan ante la comisión de esta infracción; finalmente, el último tema desarrolla el impacto que ha tenido la declaratoria de estado de emergencia luego de la pandemia por COVID-19 en el aumento del ciberdelito de clonación de tarjetas.

En el tercer y último capítulo se ofrecen informaciones acerca de la política criminal llevada a cabo en la persecución del ciberdelito de clonación de tarjeta. En este se encuentra cuáles son las entidades encargadas de la persecución, qué dificultades se

presentan con relación al manejo de la prueba, las problemáticas en la persecución debido al carácter transnacional de este tipo de delitos, la colaboración que se deben dar los países. Además, cómo se ha desarrollado el tema de la ciberseguridad en la República Dominicana.

Finalmente, aparecen las conclusiones desprendidas a raíz de los resultados alcanzados y las informaciones analizadas, así como también algunas recomendaciones que se proponen con el fin de mejorar la problemática objeto de estudio.

Para la realización de esta investigación, se hará uso del método deductivo, toda vez que, para su elaboración, se partirá de preceptos establecidos en la Constitución dominicana, como primera norma del ordenamiento jurídico dominicano, sucesivamente por Convenios internacionales ratificados por el estado, como lo es el Convenio de Budapest y, finalmente, leyes internas que regulan de manera específica el delito investigado, entre ellas la Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología en la República Dominicana.

El ciberdelito de clonación de tarjetas bancarias en la República Dominicana

Capítulo I. Aproximación al ciberdelito

Este primer capítulo está dividido en cuatro acápites. En el acápite 1.1 se desarrolla todo lo concerniente al origen y evolución del ciberdelito; en el acápite 1.2 se define y se establecen sus características. En el acápite 1.3 se pone de relieve la clasificación del ciberdelito. En el último tema, el 1.4, se despliega el marco normativo y regulatorio de los ciberdelitos y legislación aplicable tanto a nivel internacional como nacional.

1.1 Origen y evolución

Los artilugios electrónicos tales como los celulares, las computadoras, así como también la creación del internet y de sistemas digitalizados han influido bastante en los avances de la sociedad del siglo XXI y en esa misma escala, también ha ido aumentando la cantidad de ciberdelitos que ocurren cada día.

Siguiendo esa línea, podría afirmarse que la ciberdelicuencia se originó con el uso del internet, sin embargo, se ha registrado que los "primeros casos de delincuencia cibernética se llegaron a cometer incluso, antes de que el internet llegara a existir"[1], y para ese entonces estas infracciones solo eran traducidas como robo de datos. No obstante, se puede argumentar que la historia y evolución del delito cibernético van de la mano con el avance mismo del internet. Al principio, como se ha dicho, se trataba de un simple robo de información que se extraían de facturas o documentos que contuvieran la informacion personal y que, por lo general, estaban tirados en la basura. Pero en la misma medida en que el internet se fue desarrollando, asimismo pasó con los ataques.

Los ataques de delitos informáticos que llegaron con la creación y uso del correo electrónico se dieron en la década de 1980. A través de este, una gran cantidad de virus eran transmitidos a la computadora e incluso multiplicados de manera automática. Estos virus tendían a hackear el mismo correo, a ralentizar las máquinas, a dañar algunos

[1] RINALDI, Paola. ¿De Dónde Viene El Delito Cibernético? Origen Y Evolución. *Le VPN Spanish* [en línea]. 27 de abril de 2017 [consultado el 9 de marzo de 2022]. Disponible en: https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/

programas, entre otros. El uso del correo electrónico implicó la llegada de estafas tales como el *phishing* y el *malware* las cuales eran transmitidas a traves de archivos adjuntados al correo enviado.

En la década de 1990, se popularizaron los navegadores web utilizando el sistema world wide web (www). A través de estos navegadores y de las conexiones a internet, se trasmitían una serie de virus molestosos, como la conocida publicidad de sitios pornográficos, el cual se trataba de una infección con *malware*.

Fue a partir del siglo XXI, con el boom de las redes sociales, que los delitos cibernéticos comenzaron a cobrar aun más sentido. Las personas creaban perfiles en estas redes sociales e incluían y compartían gran parte de su información con un público muchas veces hasta desconocido sin saber cuáles eran las intenciones de las demás personas con las que por allí se socializaba; convirtiéndose pues, en blancos fáciles para los ladrones cibernéticos. En tal sentido, la década de 2000 no hizo sino más que aumentar la ciberdelincuencia, dada la naturaleza de estas plataformas.

Para el año 2020, fruto de la pandemia COVID_19, (que ha conseguido aislar a los seres humanos en sus hogares y recurrir a la virtualidad y los medios electrónicos o tecnológicos como herramientas de trabajo, de uso social y medio de desahogo), la ciberdelincuencia aumentó drásticamente; circunstancia que se ha venido arrastrando hasta el año en curso. La República Dominicana no ha sido ajena a este escenario, que ocurre en cualquier momento y desde cualquier lugar.

1.2 Definición y características

En la actualidad, la utilización de las TIC´s (Tecnologías de la Información y la Comunicación), se van desarrollando en conjunto a la dinámica de la vida moderna. Hoy en día todo tiene que ver con dispositivos electrónicos, aplicaciones informáticas y el uso del Internet para interrelacionarse, bien sea de forma personal o laboral o de forma pública o privada.

En contraposición al innegable avance que representa el empleo y uso de tecnologías de la información y la comunicación, debe hablarse de ciberdelitos, los

cuales además de comprender nuevos delitos se incluyen también delitos tradicionales conocidos (como los delitos de contenido: estafa, chantaje, transferencia ilícita de fondos) pero cometidos vía cibernética, de esta manera se podrán crear las consecuencias jurídicas que resultan de la particularidad de estos, por ejemplo, el problema de las múltiples jurisdicciones.

En ese contexto, surgen con los ciberdelitos, los términos delitos informáticos o delitos cibernéticos también conocidos como delitos de alta tecnología o cibercrimen. Estos conceptos, a pesar de que pueden interpretarse como que se trata de conceptos afines y/o que en algún momento se relacionen entre sí, evidencian en el fondo ciertas diferencias.

Es por ello por lo que, lo primero que se debe hacer es definir los términos: delito informático y ciberdelito, no sin antes definir el término delito. El delito es definido comúnmente como un hecho, ya sea de acción u omisión, típico, antijurídico, culpable el cual a veces es punible o sancionable. Cada una de estas características constituye los elementos necesarios para poder hablar de delito. Asimismo, hay que hacer constar que cada uno de ellos es prerrequisito del siguiente, siendo así no podemos pasar de la tipicidad a la antijuridicidad, ni de la antijuridicidad a la culpabilidad.

En esa misma línea, Téllez Valdés, ha dado "un concepto típico" de delitos informáticos estableciendo que "son las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin"[2]. La definición surge en consonancia a los elementos que forman parte de la clásica definición del delito, es decir: es un hecho, típico, antijurídico y culpable. En ese sentido, para que pueda o no sancionarse a un infractor de la ley penal informática es necesario que sea declarada su culpabilidad previamente.

Con esa base conceptual, pueden considerarse estos delitos como conductas

[2] TÉLLEZ VALDES, Julio. *DERECHO INFORMÁTICO* [en línea]. 2ª ed. Mexico: McGRAW-HILl/INTERAMERICANA DE MÉXICO, 1998. ISBN 970-10-0905-3 [consultado el 6 de marzo de 2021]. P. 187 - 188. Disponible en: https://www.bing.com/search?q=TÉLLEZ+VALDÉS,+Julio,+2009.+Derecho+informático&cvid=6285287629f84a86813f8dd1e6ddd965&aqs=edge..69i57.982j0j4&FORM=ANAB01&PC=U531.

típicas, antijurídicas e imputables, perpetradas por medios tecnológicos y sometidas a una sanción penal, siendo los más comunes, delitos contra la confidencialidad, la disponibilidad de los datos, contra los sistemas informáticos, el derecho de autor y la propiedad intelectual.

Asimismo, se puede decir que delitos informáticos son todas aquellas acciones contrarias a la ley que se ejecutan a través de la utilización de sistemas informáticos o cualquier otro componente de la comunicación y que tienen como objetivo dañar, provocar pérdidas u obstruir el correcto ejercicio de los sistemas informáticos.

En ese orden, vale precisar que una definición muy completa que existe sobre delincuencia informática es la que establece que: "[d]elincuencia informática es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera"[3] y que, independientemente que produzca un daño o no, está sancionado con una pena.

Por otra parte, y de acuerdo con el Convenio sobre la Ciberdelincuencia celebrado en Budapest en el año 2001, ciberdelitos son todos aquellos "actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, así como el abuso de dichos sistemas, redes y datos"[4].

En sentido amplio, según Marco Gercke, cabe señalar que el término "ciberdelincuencia es más restrictivo que el de delito informático, dado que implica una red informática mientras que los delitos informáticos comprenden incluso a los que afecta a sistemas informáticos autónomos, que no están conectados a una red"[5]. En ese orden, la ciberdelincuencia, puede ser definida como aquellas infracciones que mediante maniobras fraudulentas logran el borrado, deterioro, alteración o la inaccesibilidad de datos informáticos que resultan en agravio para su titular.

[3] ACURIO DEL PINO, Santiago. Delitos informáticos: generalidades. 2016. [en línea]. Ecuador. [Consultado el 2 de marzo de 2021]. P. 14. Disponible en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
[4] Consejo de Europa, Convenio Sobre la Ciberdelincuencia, Budapest. 2001.
[5] GERCKE,Dr. Marco. *Comprensión del Ciberdelito: Fenómenos, Dificultades y Respuesta Jurídica*. [en línea]. UIT, 2014. [Consultado en 17/03/2021]. P. 11. Disponible en: Libro UIT CybcrimeS | PDF | Tecnología de información y comunicaciones | La seguridad informática (scribd.com)

Sin embargo, bien pudiera decirse que el concepto ciberdelito, acuñado luego de la celebración del Convenio de Budapest, es un concepto evolucionado de los tradicionales delitos informáticos y, Urbano Castrillo citado por Quevedo Gonzales, explica que "cuando se habla de ciberdelito se hace referencia a un tipo de delito, ya sea tradicional o propio de la sociedad de la información, propiciado por las tecnologías que ésta aporta"[6]. Es decir, el ciberdelito se refiere a cualquier actividad ilegal llevada a cabo simplemente mediante el uso de tecnología mientras que los delitos informáticos pueden ser todos los hechos delictivos cometidos mediante un dispositivo informático (computadora, celular, Tablet, entre otros) como medio para obtener un fin ilícito.

Evidentemente, también se puede colegir, que el término ciberdelincuencia o ciberdelito es utilizado más como un término genérico que engloba acciones delictivas ejecutadas a través del uso de equipos informáticos o internet y que en tal sentido ambas van de la mano.

Dentro de los ciberdelitos sobresalen los siguientes como los más comunes:

- *Phishing* (suplantación de identidad con el fin de obtener datos de forma fraudulenta).
- *Grooming* (acercamiento de un adulto a un menor por medio del ciberespacio con fines de abuso sexual).
- *Cyberbulling* (acoso psicológico entre iguales).
- *Pharming* (vulnerabilidad a sistemas DNS).
- *Ciberstalking* (persecución o acoso a traves de Internet u otros medios electrónicos).
- *Sextorsion* o extorsión sexual (extorsión con amenaza de divulgar imágenes privadas).

Otra forma en la que se puede definir el concepto ciberdelito es a partir de lo que supone el o los delitos transnacionales. El delito trasnacional es aquel en donde, además de violarse el derecho interno de un país, se viola también el derecho internacional tales

6 QUEVEDO GONZÁLEZ, Josefina. *INVESTIGACION Y PRUEBA DEL CIBERDELITO*. Maestría, Universidad de Barcelona, 2017 [consultado el 16 de abril de 2021]. P.11. Disponible en: http://diposit.ub.edu/dspace/bitstream/2445/128112/1/JQG_TESIS.pdf

como, el blanqueo, la trata de personas, y el narcotráfico. Es decir, que se lesionan bienes jurídicos comunes y a la vez protegidos en diferentes países, dando paso a la figura conocida como crimen organizado, para los efectos de esta, ciberdelincuencia organizada.

Y, a pesar de que, según el Compendio De Ciberdelincuencia Organizada, hecho por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), establece que "no hay consenso sobre la definición de ciberdelincuencia organizada"[7]; el mismo compendio, para sus efectos, define a la ciberdelincuencia organizada como aquellos delitos basados o facilitados por la cibernética y que son cometidos por un grupo delictivo organizado[8]. Los ciberdelincuentes que conforman estos grupos, son aquellas personas que perpetran los cibercrímenes.

El cibercrimen es un acto ilícito que tiene como objetivo los dispositivos digitales o es cometido vía Internet, computadoras o tecnología relacionada. De esta manera, hay dos opciones claras: crímenes tradicionales que utilizan el ciberespacio como medio o crímenes totalmente nuevos que solo se pueden perpetrar en el ciberespacio. Todo ello también tiene que ver con las características de los cibercriminales, donde hay cibercriminales que son puros técnicos (hackers/crackers) y cibercriminales que utilizan los medios tecnológicos para perpetrar delitos tradicionales (robos, fraudes, acoso, tráfico de drogas,…), y aquí hay que poner el acento en una modalidad en auge, según EUROPOL, como lo es el cibercrimen como servicio (crime as a service), es decir, diferentes hackers (de sombrero negro) que ponen a disposición de cualquier persona que quiera pagar kits para poder cometer ciberdelitos, desde consolas de bots para perpetrar ataques DoS, hasta completos paquetes para crear webs y hacerse con credenciales personales bancarias (phishing).

Por ejemplo, en los delitos de fraudes que se perpetran a través de software tales como: Adware (programas que compilan información sobre hábitos de navegación de los usuarios para luego mostrar publicidad); programas de acceso remoto (a través de los cuales una tercera persona puede acceder a un ordenador para luego proceder al

[7] OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO. Compendio de Ciberdelincuencia Organizada, Viena, 2022. [en línea]. [consultado el 10 de abril de 2022]. P.3. Disponible en: https://www.unodc.org/documents/organized-crime/tools_and_publications/21-05345_S_eBook.pdf
10 *Ibidem*

ataque); caballos de Troya o Troyanos (virus que se identifican por engañar a los usuarios haciéndoles creer que son programas o archivos benignos y cuya finalidad es infectar y causar daño); programas de espionaje o spyware (que recopilan la información que se realiza en una computadora para después transmitirla a una entidad externa sin autorización del propietario); virus o gusanos (worms) (son programas maliciosos que se infectan a otros ordenadores a través del correo electrónico, entre otros..) se provocan daños en el sistema informático, tales como que los datos sean alterados o borrados.

En ese tenor, y tomando en cuenta el uso indistinto de los diferentes términos, se infiere que estos tipos de actividades que comprenden la realidad virtual, a pesar de ser muy variadas, poseen algunas características que las acompañan de forma recurrente. Entre ellas se encuentra que siempre se ejecutan mediante programas o aplicaciones maliciosas que persiguen dañar, alterar, borrar o suprimir datos informáticos sin el permiso o excediendo el permiso que le haya sido otorgado por el dueño.

Otra característica es que estos comportamientos criminales, en su generalidad, son cometidos por personas con conocimientos especiales, en este caso, personas aptas que tienen competencias y habilidades en el ámbito de la ingeniería social. Por lo que, en la mayoría de los casos, son calificados como delitos dolosos pese a que también muchos se cometen de forma imprudencial. Sin embargo, respecto al perfil del cibernético también ha habido ciertas transformaciones porque el ciberdelincuente ya no es la típica persona descrita más arriba, sino que se trata de individuos que, así como han evolucionado los delitos, de igual manera evolucionan ellos, de ahí que aunque conocen de crímenes tradicionales, ahora se valen de las tecnologías para llevar a cabo el ilícito. Es común también que estas personas obtengan conocimientos a través del intercambio de información con extranjeros que conozcan sobre este tipo de hechos.

Otra particularidad es que pueden suponer pérdidas cuantiosas de dinero, no solo a nivel personal o comercial sino también a nivel mundial. De esto se concluye que los ciberdelitos son delitos de mera actividad porque no requieren un resultado o daño, basta con que se haya ejecutado la acción y la permanencia del hecho, porque se puede dar varias veces en el tiempo.

Y finalmente, suponen ser delitos pluriofensivos toda vez que pueden verse afectados más de un bien jurídico protegido a la misma vez. Así como también que, por ser delitos trasnacionales, presentan dificultades para ser perseguidos y comprobados ya sea tomando en cuenta la ubicación (ya que se realizan de forma remota y muchas veces desde diferentes ciudades, países) o también, de acuerdo con el nivel de equipos, instrumentos y destrezas que posea el ciberdelincuente puesto que se dificultará el rastreo.

En resumen, los delitos tradicionales se entrelazan fácilmente a los tecnológicos. Estos son delitos que se sitúan rápidamente en los ámbitos geográficos nacionales e internacionales, donde no importa el lugar donde este el autor ni la víctima, ya que, estas conductas se ejecutan de forma instantánea y, en las mayorías de los casos, mientras el ciberdelicuente ejecuta el acto delictivo, este le pasa totalmente desapercibido a la víctima.

Las evidencias que demuestran o comprueban que fue cometido un delito informático, no se guardan por largos periodos de tiempo; es un hecho que afecta intereses económicos, sociales, políticos, etc. Y la pena es muy ínfima para la gravedad de los daños que le ocasiona a una víctima.

En la búsqueda de contrarrestar la ciberdelincuencia surgen los sistemas de seguridad informática, los cuales son definidos como la planeación de ciberseguridad que imposibilita el acceder sin autorización a los diferentes sistemas de información tanto a la de una organización como a la de un individuo buscando mantener la confidencialidad de lo antes mencionado. Asimismo, para dar una respuesta eficiente y en tiempo hábil, se hace necesario capacitar a un personal policial y judicial con vastos conocimientos técnicos y profesionales.

1.3 Clasificación del ciberdelito

La acepción “ciberdelito” comprende varios tipos de delitos los cuales a su vez abarcan diversos tipos de infracciones. Como consecuencia, resulta ser un tanto problemático hacer una clasificación de estos llegando a existir múltiples clasificaciones de los ciberdelitos.

Por su parte, menciona Graciela Encalada Ochoa en su tesis sobre Criminalidad informática, que la Organización de las Naciones Unidas reconoce cuatro tipos de delitos informáticos[9]. La primera clasificación la denomina fraudes cometidos mediante manipulación de computadoras[10]. Esta categorización abarca la manipulación de datos de entrada, como el robo de datos; la manipulación de datos de salida, como la clonación de tarjetas; la manipulación de programas, como la inserción de programas encubiertos para que realicen funciones no autorizadas concomitantemente a su función normal; y, el fraude efectuado por manipulación informática, bajo la cual periódicamente se extraen transacciones financieras de una cuenta para transferirla a otra.

La segunda clasificación la designa como falsificaciones informáticas y la subdivide en delitos informáticos como objeto y delitos informáticos como instrumentos. En la primera subdivisión de delitos informáticos se alteran datos de la documentación archivada en forma digital. Por su parte, en la subdivisión de delitos informáticos como instrumentos son los aparatos electrónicos los que se utilizan para perpetrar las falsificaciones.

Esta clasificación va de la mano con una de las definiciones dadas anteriormente, según la cual se hace tomando en cuenta el uso de sistemas informáticos como instrumento o medio o como fin u objetivo. Dicho de otra manera, cuando las acciones delictivas se cometen a través de una computadora se dice que se utilizan los dispositivos electrónicos como medio de comisión, es decir, instrumento, sin embargo, cuando estas acciones se dirigen hacia las computadoras, sus accesorios o programas pasan pues a ser el objetivo.

La tercera clasificación que tiene que ver con dañar o modificar programas o datos computarizados se encuentra el sabotaje informático: borrado, retención o modificación, sin permiso, de datos digitales o funciones de la computadora con el fin de entorpecer el funcionamiento del sistema.

[9] ENCALADA OCHOA, Graciela. *A CRIMINALIDAD INFORMÁTICA: PROPUESTA PARA LA TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS EN LA LEGISLACIÓN ECUATORIANA*. Maestría, Cuenca, 2010 [consultado el 16 de abril de 2022]. P. 30. Disponible en: tm4328.pdf
[10] *Ibidem*

Finalmente, la cuarta categoría se encuentran aquellos hechos casos que van desde simples casos de piratería hasta el espionaje informático de ahí que, se identifiquen por lograr acceder sin autorización previa de su titular a servicios y sistemas informáticos.

En ese mismo orden, el Convenio sobre Ciberdelincuencia, clasifica los ciberdelitos en cuatro grandes grupos: Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; Delitos informáticos, Infracciones relativas al contenido, Infracciones vinculadas a la propiedad intelectual y los derechos afines[11].

Asimismo, y según el mencionado convenio, los delitos pueden clasificarse también en función del bien jurídicamente protegido, aquí se encuentran:

- Delitos de internet que afectan la intimidad.
- Delitos contra la libertad e indemnidad sexual.
- La afectación de la propiedad (como la propiedad intelectual y derechos de autor).
- Delitos que atentan contra la nación y actos de terrorismo (que afectan la seguridad nacional).

La Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología en la República Dominicana en ese sentido, asume en su contenido la clasificación que se hace en el Convenio sobre Ciberdelincuencia.

En ese tenor, y respecto a la primera clasificación: delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos[12], se encuentran infracciones tales como: divulgar códigos de acceso, la clonación; el acceso ilícito; el uso de dispositivos fraudulentos; la alteración de datos y el sabotaje, entre otros.

[11] Consejo de Europa, Convenio Sobre la Ciberdelincuencia, Budapest. 2001.
[12] REPÚBLICA DOMINICANA. Congreso de la Republica Dominicana. Sobre Crímenes y Delitos de Alta Tecnología [en línea]. Ley n.º 53-07 de 23 de abril de 2007 [consultado el 10 de enero de 2022]. Disponible en: https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf

En cuanto a la segunda categoría (los delitos de contenido), esta abarca los contenidos que se consideran ilegales, tales como: atentado contra la vida de la persona, el robo, la obtención ilícita de fondos y la transferencia electrónica de fondos, la estafa, el chantaje, el robo de identidad, la falsedad de documentos y firmas[13]. Asimismo, el comercio ilícito a través del Internet o de cualquier otro sistema de información, el tráfico ilícito de humanos o migrantes, el atentado sexual, la difamación y la pornografía infantil, entre otros.

En lo que respecta a la tercera clasificación se encuentran los delitos relacionados a la propiedad intelectual. En esta se incluyen las infracciones establecidas en la Ley No.20-00, del 8 de mayo del año 2000, sobre Propiedad Industrial[14], y la Ley No.65-00, del 21 de agosto del año 2000, sobre Derecho de Autor[15].

Debe hacerse énfasis en que para estar presentes ante un denominado ciberdelito, todas estas infracciones deben ser realizadas a través de la utilización de sistemas informáticos, telemáticos, de telecomunicaciones, electrónica o audiovisual.

Una cuarta categoría abarca los delitos contra las telecomunicaciones la cual, a su vez, comprende infracciones tales como: llamada de retorno de tipo fraudulento, el fraude realizado por proveedores de servicio de información, el redireccionamiento de llamadas de larga distancia, el robo de línea, el desvío de tráfico a través de rutas no autorizadas, la manipulación ilícita de equipos de telecomunicaciones y, la intervención de centrales privadas[16].

Finalmente, se puede decir que existe en la República Dominicana una quinta categoría que es la que abarca aquellos crímenes o delitos cometidos en contra de La

[13] REPÚBLICA DOMINICANA. Congreso de la Republica Dominicana. Sobre Crímenes y Delitos de Alta Tecnología [en línea]. Ley n.º 53-07 de 23 de abril de 2007 [consultado el 10 de enero de 2022]. Disponible en: https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf.

[14] REPÚBLICA DOMINICANA. Congreso de la Republica Dominicana. Sobre Propiedad Industrial [en línea]. Ley n.º 20-00 de 8 de mayo de 2000 [consultado el 10 de enero de 2022]. Disponible en: doi:file:///C:/Users/Usuario/Downloads/ley20-00.pdf

[15] REPÚBLICA DOMINICANA. Congreso de la Republica Dominicana. Sobre Derecho de Autor [en línea]. Ley n.º 65-00 de 26 de julio de 2000 [consultado el 10 de enero de 2022]. Disponible en: https://www.aduanas.gob.do/media/2213/65-00_sobre_derecho_de_autor.pdf

[16] REPÚBLICA DOMINICANA. Congreso de la Republica Dominicana. Sobre Crímenes y Delitos de Alta Tecnología [en línea]. Ley n.º 53-07 de 23 de abril de 2007 [consultado el 10 de enero de 2022]. Disponible en: https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf

Nación, así como de Actos de Terrorismo. Respecto a los Crímenes y Delitos contra la Nación, el artículo 27 de la Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología, los define como aquellos "actos que se realicen a través de un sistema informático, electrónico, telemático o de telecomunicaciones, que atenten contra los intereses fundamentales y seguridad de la Nación, tales como el sabotaje, el espionaje o el suministro de informaciones"[17].

Por su parte, el artículo 28 condena los actos de Terrorismo, al establecer que "todo aquel que, con el uso de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, ejerza actos de terrorismo, será castigado con pena de veinte a treinta años de reclusión y multa de trescientos a mil salarios mínimos, del sector público. Asimismo, se podrá ordenar la confiscación y destrucción del sistema de información o sus componentes, propiedad del sujeto pasivo utilizado para cometer el crimen"[18].

1.4 Marco normativo y regulatorio: legislación aplicable

En el presente apartado se desarrolla el marco regulatorio de los delitos informáticos y la legislación aplicable al ciberdelito en el ámbito internacional, así como los tratados internacionales aprobados y ratificados por el país y la normativa objetiva.

1.4.1 A nivel internacional

A nivel internacional, la protección contra delitos cibernéticos ha sido estipulada en el Convenio de Budapest, también conocido como el Convenio de Budapest sobre ciberdelincuencia[19], elaborado durante el 2001 por el Consejo de Europa, de cuyo convenio la República Dominicana es signataria, desde el 7 de febrero 2013.

El Convenio de Budapest constituye el único tratado internacional vinculante en materia de ciberdelitos comprendiendo una especie de brújula para que los Estados partes puedan: a) armonizar sus leyes penalizando las infracciones realizadas a través de medios informáticos, (derecho penal sustantivo); (b) regular normas procesales que

[17] Ob.cit..
[18] Ob.cit.
[19] Ley de Ciberseguridad se adheriría a Convenio de Budapest sobre ciberdelincuencia. Noticias Cholusat Sur [en línea]. [sin fecha] [consultado el 8 de julio de 2022]. Disponible en: http://cholusatsur.com/ley-de-ciberseguridad-se-adheriria-convenio-de-budapest-sobre-ciberdelincuencia/

sistematicen el poder detectar a tiempo, investigar y perseguir de forma eficaz estas infracciones, (derecho penal adjetivo) y (c) prever una práctica positiva y segura de cooperación internacional que procure erradicar la criminalidad en el ciberespacio. Es decir, el Convenio procura, con la activa participación de los Estados involucrados, combatir la comisión de delitos informáticos o de los delitos en Internet a través del ajuste y concierto de leyes nacionales, el mejoramiento en los procesos de investigación y el fortalecimiento de la cooperación que debería existir entre los países.

En ese sentido, la adhesión a este convenio habilita consecuencias bilaterales en la ardua lucha que implica la prevención, persecución y represión del ciberdelito sobre todo en los aspectos que faciliten su persecución. La acentuación de la cooperación internacional se comprueba a través de la realización de programas de intercambio de conocimiento, la intervención o cooperación en la ejecución de acciones en conjunto con diferentes países, la eficaz cooperación en el proceso de investigaciones, la asistencia en el manejo de la evidencia digital, así como en las ventajas que naturalmente emanan del proyecto "Acción global contra el ciberdelito ampliada" conocido como GLACY + por sus siglas en inglés[20].

El Convenio de Budapest consta de varios títulos. En el título I se encuentran desglosados los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. En el título II están las infracciones informáticas. En el título III, todas aquellas infracciones relativas al contenido (en este renglón encontramos delitos tradicionales pero que son cometidos mediante el uso de sistemas informáticos o telemáticos) y, finalmente en el título IV encontramos las infracciones relativas a la propiedad intelectual y al derecho de autor.

Es preciso destacar que aunque el convenio ha sido ratificado por 66 países, en Latinoamérica, únicamente la República Dominicana, Costa Rica, Chile y Argentina han establecido la Red 24/7 prevista en el Artículo 35 del Convenio de Budapest como órgano central de asesoramiento vinculado con la Fiscalía y los organismos de investigación policial para garantizar la asistencia jurídica inmediata relacionada con investigaciones penales en el contexto tecnológico y/o para solicitar pruebas contenidas

[20] Council of Europe (2020) en CASTILLO RUBIANO, Oscar. (2021). Phishing: Día de Pesca. Colombia.

en formato electrónico a otras autoridades a través de las redes de contacto de los 66 países que forman parte del Convenio de Budapest[21].

Por otra parte, otra resolución que constituye una estrategia integral para prevenir el delito cibernético a través de la ciberseguridad es la Resolución AG/RES 2004 (XXXIV- O/04) de la Asamblea General de la Organización de los Estados Americanos aprobada el ocho (08) de junio de 2004. Esta resolución contempla modalidades de acción para la adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética y un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética[22].

De carácter regional está la Ley modelo sobre el delito cibernético - Commonwealth of Nations, la cual es relevante porque enfrenta procedimientos para tratar una problemática mundial estableciendo medidas que funcionan como guía o patrón para otras naciones, es decir que, esta normativa implica una gran influencia a nivel internacional respecto a las investigaciones sobre el desarrollo del ciberdelito, lo que supone que herramientas con estas particularidades "están diseñados para servir como inspiración o 'modelos' para el desarrollo de disposiciones legislativas nacionales. (…) los instrumentos no vinculantes pueden tener una influencia enorme a nivel global o regional cuando muchos estados deciden alinear sus leyes nacionales (...)" [23].

En otro orden, en julio de 2019 se celebró en el Salvador, la XII Reunión de la Comisión Interparlamentaria de Seguridad Ciudadana y Administración de Justicia y la IX Reunión de la Comisión Interparlamentaria de Asuntos Internacionales e Integración del Foro de Presidentes de Poderes Legislativos de Centroamérica y la Cuenca del Caribe (FOPREL), a través de la cual el Consejo de Europa mediante el Proyecto GLACY +, y los países miembros del FOPREL (Belice, Costa Rica, El Salvador,

[21] MEDINA RUVALCABA, Estefanía; San Martin, Cristos Velasco y Velázquez Olavarrieta, Andrés Recomendaciones para abordar la detección e investigación del fraude cibernético en México. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1057296/fraude_cibernetico.pdf

[22] Resolución AG/RES. 2004 (XXXIV-O/04) de 8 de junio de 2004 - Informática Jurídica. *Informática Jurídica* [en línea]. 28 de abril de 2021 [consultado el 10 de junio de 2022]. Disponible en: https://www.informatica-juridica.com/resolucion/resolucion-ag-res-2004-xxxiv-o-04-de-8-de-junio-de-2004/#:~:text=Resolución%20AG/RES.%202004%20(XXXIV-O/04)%20de%208%20de%20junio,una%20cultura%20de%20Seguridad%20Cibernética.%20AG/RES.%202004%20(XXXIV-O/04)

[23] Oficina de Naciones Unidas contra la Droga y el Delito UNODC, 2013, p. 72.

Guatemala, Honduras, Nicaragua, México, Panamá, Puerto Rico y República Dominicana) aprobaron una resolución que exhorta y vincula a los países partes la aprobación de legislar en materia del ciberdelito de manera que se pueda combatir eficientemente y además, establecer las medidas correctas que faciliten su identificación, investigación y persecución y sanción así como también para temas de cooperación internacional. Cabe decir que la Republica Dominicana desde febrero de 2013 forma parte del Convenio de Budapest y cuenta con una legislación independiente para investigar, perseguir y sancionar delitos cibernéticos: la Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología vigente desde el 2007.

1.4.2 En República Dominicana

El marco jurídico de la República Dominicana está conformado en primer lugar por la Constitución Política Dominicana, luego de manera específica por la Ley No. 53-07 Sobre Crímenes y Delitos de Alta Tecnología, así como también otras leyes complementarias.

Se debe comenzar por la Constitución Dominicana, ya que es la norma fundamental en que descansa todo el ordenamiento jurídico del Estado dominicano, a través de esta toda norma que se introduzca no debe, ni en su forma ni en su contenido, estar por encima o entrar en choque con lo que establece La Constitución, por lo tanto, se debe de acentuar que la Constitución es un conjunto integral de preceptos que no se pueden analizar de manera aislada o separada de las otras leyes de la República.

Respecto al artículo 44 de la Constitución, Sosa Pérez dice que: "El derecho a la intimidad establece límites para la protección a la vida privada de la persona. La intimidad está constituida por un conjunto de comportamientos, datos y situaciones que pertenecen a una persona y que deben estar sustraídos al conocimiento de extraños... El derecho a la intimidad es aquella facultad que tienen las personas a tener un espacio propio personal, una esfera privada de su vida, inaccesible al público salvo expreso consentimiento del interesado"[24].

[24] SOSA PÉREZ, Rosalia**,** Comentarios al Derecho a la Intimidad y el Honor Personal, Constitución Comentada, Finjus, Segunda Edición, 2012, p. 110

Este mismo artículo 44 de la Constitución, pero en su apartado 2, protege los datos personales de todos los individuos y lo consagra como un derecho fundamental; el texto establece que todas las personas tienen derecho de saber sobre los datos que sobre su persona se encuentren en registros tanto públicos como privados, y también saber cuál es el uso que se le dará a los mismos. Además de la Constitución, el derecho a la protección integral de los datos personales se encuentra amparado en la Ley No. 172-13 promulgada el 13 de diciembre del año 2013; la cual, además, busca que el derecho al honor y a la intimidad también sea garantizado.

Este derecho a proteger la información personal de los dominicanos viene recogido en preceptos establecidos en pactos internacionales, de los cuales el país ha sido signatario y que, como consecuencia, debe aplicar. Dentro de estos encontramos la Declaración Universal de los Derechos Humanos, adoptada por la Asamblea General de Naciones Unidas, la cual en el artículo 12, establece que: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Por otra parte, del mismo modo se recoge en el Pacto Internacional de Derechos Civiles y Políticos, adoptado también por la Asamblea General de Naciones Unidas, en su artículo 17 literal d, lo siguiente: "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación". Y, "2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

Como consecuencia, y al ser la República Dominicana signataria de estos pactos, debe ajustarse al cumplimiento de estos mandatos y dirigir políticas en ciberseguridad respecto a las informaciones personales de las personas y que figuren en el ciberespacio; procurando, además, proteger y resguardar para así evitar que se afecten bienes jurídicos protegidos de los ciudadanos. De la única manera en que una información personal debería utilizarse es solo si se hace en beneficio del individuo, pero nunca para atentar contra su dignidad o con fines de discriminación o negocio, como sucede en los casos de venta de informaciones crediticias para la red oscura.

En otro orden, tras el desarrollo del internet y las altas tecnologías y concomitantemente a esto, los nuevos tipos delictuales que surgen a partir de los avances informáticos y tecnológicos, así como de la creación del Convenio de Budapest, surge la obligación de que el país se tuviera que actualizar y creara nuevos tipos penales para así proteger el derecho constitucional a la intimidad, la propiedad, la intelectualidad, la comunicación, entre otros.

En consecuencia, el 23 de abril del 2007 se promulga una ley exclusiva para tipificar y sancionar de manera particular estos delitos especiales, ya que en el Código Penal Dominicano no se encontraban penalizados como tal los ciberdelitos o los delitos informáticos. Es así como surge la Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología, "concepto este que en otras legislaciones como las de Colombia, Perú, Venezuela y Chile fue adoptado con el nombre de Delitos Informáticos"[25]. La promulgación de esta ley nos coloca en el estándar de protección de datos, de sistemas de información y de la intimidad.

Esta norma jurídica sirve de marco de protección contra los ciberdelitos que se cometan tanto en perjuicio de personas físicas como morales, la cual contiene en su interior no solamente las tipificaciones penales respecto a hechos perpetrados mediante medios tecnológicos y sus respectivas sanciones; sino que crea una serie de organismos de regulación y control para su persecución y su prevención.

En ella, el legislador clasifica las infracciones en varias categorías: "a) crímenes y delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas de información; b) delitos de contenido; c) delitos de propiedad intelectual y afines; d) delitos contra las telecomunicaciones; e) crímenes, delitos contra la nación y actos de terrorismo"[26].

[25] ROMERO PÉREZ, Hector Manuel. *Análisis de Los Crímenes y Delitos de Alta Tecnología en el Distrito Nacional, 2007-2013*. En: https://bibliotecaunapec.blob.core.windows.net/tesis/TPG_CI_MDP_48_2013_ET140182.pdf [base de datos en línea] [consultado el 15 de mayo de 2022]. Tesis de postgrado, Universidad APEC, 2013. P. 25. Disponible en: https://bibliotecaunapec.blob.core.windows.net/tesis/TPG_CI_MDP_48_2013_ET140182.pdf

[26] REPÚBLICA DOMINICANA. Congreso de la Republica Dominicana. Sobre Crímenes y Delitos de Alta Tecnología [en línea]. Ley n.º 53-07 de 23 de abril de 2007 [consultado el 10 de enero de 2022]. Disponible en: https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf

En esa misma tesitura, resulta importante señalar que para la creación de la Ley 53-07, sobre Crímenes y Delitos de Alta Tecnología, se utilizaron como referencia otras leyes que tipifican ciertas conductas ilícitas pero que bajo el amparo de esta ley, deben siempre cometerse mediante el uso de sistemas informáticos o telemáticos.

Tal es el caso, por ejemplo, del Código Penal Dominicano en el cual se tipifican delitos como el robo y la estafa; la Ley 136-03, que crea el Código para el Sistema de Protección y los Derechos Fundamentales de Niños, Niñas y Adolescentes, respecto a infracciones donde estén envueltos menores de edad; la ley No. 153-98, General de Telecomunicaciones, la cual prohíbe el uso de las telecomunicaciones para cometer delitos; la Ley No. 20-00, del 8 de mayo del año 2000, sobre Propiedad Industrial, y la Ley No. 65-00, del 21 de agosto del año 2000, sobre Derecho de Autor, respecto a infracciones concernientes a la Propiedad Intelectual y Afines siempre que se cometan a través del empleo de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o de cualquiera de sus componentes.

Capítulo II. La clonación de tarjetas bancarias

En este segundo capítulo se detalla de manera específica todo lo relacionado con el ciberdelito de clonación de tarjetas. Este apartado está dividido en cinco subtemas; en el subtema 2.1 se comienza explicando qué es una tarjeta bancaria para de allí, pasar al subtema 2.2 y poder explicar qué es clonación de tarjeta y a su vez cómo se tipifica y sanciona en la República Dominicana. En el tema 2.3 se detallan cuáles son los diferentes métodos utilizados por los ciberdelincuentes para clonar tarjetas, y como una subsección a este se desarrollan cuáles derechos y libertades se afectan ante la comisión de esta infracción; finalmente, en el último tema, el 2.5, se desarrolla el impacto que ha tenido la declaratoria de estado de emergencia luego de la pandemia por COVID_19 en el aumento del ciberdelito de clonación de tarjetas.

2.1 ¿Qué es tarjeta bancaria?

Es considerable establecer que el avance y evolución respecto al uso del dinero en moneda y papel hacia el uso de tarjetas, ya sean de crédito o de débito, como forma de pago, han significado un gran desarrollo para las sociedades, además, de seguridad para los ciudadanos. Debido a que, con el uso de tarjetas, o papel plástico, como también es

denominado, las personas salen a las calles sin el miedo a ser atacadas y a que su dinero en efectivo le sea robado ya que, con una simple llamada al banco se puede bloquear la tarjeta para que esta no pueda ser usada.

Las tarjetas, ya sea de débito o crédito, son dispositivos que forman parte del diario vivir de una gran parte de los seres humanos por la comodidad que presenta su uso, y a su vez, evita que se tenga que cargar con sumas importantes de dinero, que es lo que le gustaría a los estafadores. Sin embargo, conforme las cosas y las sociedades han ido evolucionando, asimismo aumentan significativamente los riesgos ante los cuales los usuarios del internet se ven expuestos al exhibir sus datos en la red.

De tal modo que, la tranquilidad de usar tarjetas rápidamente desapareció tras ganar notoriedad la delincuencia informática, puesto que se pueden cometer una serie de ilícitos que afectan las informaciones personales y crediticias del usuario de la red, y que al final se traducen en la afectación de cada persona o de su patrimonio. Dentro de estos ciberdelitos a los que hay que estar asechos se encuentran: la clonación de tarjetas y cuentas bancarias, la transferencia de fondos, y las compras y estafas en línea.

No obstante, antes de comenzar a desarrollar el concepto y las características propias respecto a la clonación de tarjetas, se hace imprescindible en primer lugar, hablar sobre lo que es una tarjeta bancaria.

Una tarjeta bancaria puede ser definida como aquella forma de pago expedido por una entidad financiera a un consumidor luego de cumplirse la formalidad de un contrato firmado tanto por el consumidor como por la entidad bancaria. Su objetivo principal es permitir el retiro de dinero a través de cajeros automáticos o en su defecto poder pagar o comprar ya sea en tiendas físicas como en línea, sin la necesidad de tener dinero en efectivo en ese momento.

Hay muchos tipos de tarjetas bancarias en el mercado financiero, sin embargo, la clasificación más genérica es aquella que las categoriza como: tarjetas de crédito y tarjetas de débito. Las tarjetas de débito son aquellas mediante las cuales se puede comprar y pagar en los diferentes establecimientos comerciales y de servicios que

acepten esta forma de pago, asimismo hacer retiros en efectivo del dinero disponible en la cuenta de ahorros a la que esté asociada la tarjeta.

Por otra parte, con la tarjeta de crédito también se realizan compras, se pagan servicios y se pueden realizar retiros en efectivo con la diferencia que esta viene asociada a una línea de crédito o préstamo, que la entidad bancaria pone a disposición del consumidor y cuyo límite dependerá de la capacidad adquisitiva o solvencia económica del consumidor. "Sin embargo, lo más característico del sistema es que no se trata de una relación intuitu personae, puesto que la deuda nace y produce plenos efectos jurídicos, aunque quien use la tarjeta no sea el titular"[27].

En este apartado de clasificación de las tarjetas bancarias, se hace necesario hacer referencia a otro tipo de tarjetas, que son las tarjetas prepagadas. Bajo esta clasificación, se le carga al titular de la tarjeta (o el mismo titular carga) una suma de dinero que posteriormente es utilizada para realizar compras de bienes o pago de servicios.

Es decir, estas tarjetas a diferencia de las anteriores, no tiene que estar asociada a una cuenta bancaria y tienen un límite de consumo que dependerá de lo que el tarjetahabiente o un tercero (como en el caso del gobierno para los beneficiarios de las Tarjetas de Solidaridad o Supérate) hayan dispuesto en ella.

En base a estas puntualidades, puede decirse que la naturaleza de las tarjetas bancarias es particularmente comercial, es decir, es una forma especializada de endosar deudas y que, estas nacen como una forma de facilitar las transacciones mercantiles entiéndase, la compra de bienes y servicios, en una era en donde se ha preferido utilizar el papel plástico, es decir, las tarjetas como medios de pago, puesto que, estas provocan una mayor actividad en los sistemas económicos y financieros de las distintas sociedades, esto sin mencionar las ventajas que a nivel personal también poseen, pues si el ciudadano sabe manejarse con ella, puede incluso utilizarla como un método de ahorro personal y de seguridad.

[27] . BATUECAS CALETRIO, A. (2005). Pago con tarjeta de crédito. Naturaleza y régimen jurídico. Cizur Menor: Aranzadi. Pág. 185

2.2 ¿Qué es clonación de tarjetas?

Siguiendo esa línea, los delincuentes, quienes no tardaron en identificar formas sobre cómo poder disponer del dinero que ahora se encontraba en un plástico, iniciaron la comisión de varias prácticas fraudulentas, entre ellas una mediante la cual se dobla, copia o plagia la información almacenada en tarjetas bancarias, valiéndose de inventivas ya sean digitales o físicas, y así poder realizar transacciones financieras ilegales y sin autorización del usuario afectado. Este método puntualizado precedentemente es lo que se ha denominado como clonación de tarjeta, la cual a nivel mundial, afecta cada año a muchas personas.

Este tipo de prácticas fraudulentas es muy común y con ella lo que se trata es de duplicar la información almacenada en tarjetas de crédito o débito haciendo uso de diversos métodos y con el objetivo de realizar operaciones financieras ilegales afectando al usuario titular.

La clonación de tarjeta es un tipo de estafa con la que las entidades financieras vienen batallando hace tiempo debido a su naturaleza, ya que para su ejecución no se requiere el uso de la fuerza, se completa de manera silente y ni el usuario, ni la entidad son conscientes de que han sido afectados hasta que se produce un consumo no reconocido y el usuario procede a reportar dicha anomalía.

Los protagonistas de esta acción ilegal muchas veces son individuos con conocimientos en informática y electrónica, los cuales ejecutan un software capaz de sustraer la información, por medio de instrumentos electrónicos normalmente basados en tecnología bluetooth diseñados para este fin.

Según se define en el Servicio Nacional del Consumidor (SERNAC): “clonar una tarjeta de crédito es extraer la información contenida en su banda magnética y copiarla en otra tarjeta con el propósito de cometer un fraude”[28]. Asimismo, se debe tener presente que el delito de clonación es una infracción cometida por grupos, en lo que cada una de las personas que lo integran tienen un rol específico dentro del conjunto

[28] SERNAC (2022). Glosario para entender fraudes tecnológicos. Disponible en: https://www.sernac.cl/portal/607/w3-article-3259.html

de actividades que son llevadas a cabo para alcanzar con su cometido. Por lo general, "el afectado se suele dar cuenta después que los gastos se han realizado"[29].

Se puede apreciar que la clonación de tarjetas bancarias constituye una especie de robo más moderna, actual y acorde a los nuevos tiempos, en la cual no se requiere ejercer ningún tipo de violencia para obtención del dinero, basta con que los malhechores tengan ciertos conocimientos informáticos para cometer la conducta típica y antijurídica. La conducta se perpetra debido a que en los últimos años "se han desarrollado nuevos sistemas informáticos y tecnológicos, en donde se pueden descifrar los códigos de seguridad de algunas tarjetas bancarias, y con esto se pueden cometer nuevas conductas antisociales como la clonación de tarjetas bancarias"[30]. Como se ha establecido, paralelamente a la evolución de las tecnologías también lo hacen los delincuentes, creando a su vez nuevas formas de delinquir.

Jaramillo Acevedo & Zambrano, han establecido que los ciberdelincuentes realizan el proceso de clonación de una tarjeta, de manera general en tres etapas. En la primera de ellas, la víctima realiza un pago en un establecimiento comercial y al perder de vista su tarjeta, el empleado que tiene la tarjeta en su poder pasa la banda de la tarjeta por un mini aparato llamado skimmer (dispositivo preparado para leer y recopilar los códigos de las bandas magnéticas de las tarjetas para su posterior descarga). En la segunda etapa se descarga la información contenida en el skimmer a una computadora y desde esta se graba la información a la cinta magnética de otros plásticos en blanco, pero, a las cuales posteriormente se le dará la apariencia de una tarjeta legítima o, se usa para sobrescribir datos a una tarjeta que previamente ya fue robada. Finalmente, en la tercera etapa, con el plástico ya terminado, es decir, la tarjeta clonada, pero con apariencia verdadera o legítima, una persona la utiliza como medio de pago en cualquier punto de venta de bienes o servicios. En algunas ocasiones, los productos comprados se comercializan más adelante para dar una apariencia más legítima al dinero y "hacer

[29] Oficina De Las Naciones Unidas Contra la Droga y El Delito. (UNODOC). Compendio de casos de delincuencia organizada.
[30] La investigación que realiza el criminólogo-criminalista en la clonación de tarjetas bancarias. P. 46. http://revista.cleu.edu.mx/new/descargas/1301/articulos/03_La_investigacion_que_realiza_el_criminologo-criminalista_en_la_clonacion_de_tarjetas_bancarias.pdf

efectivas las ganancias de todos los que intervienen en el proceso"[31].

Existe una gran variedad de modalidades delictivas que se pueden llevar a cabo mediante la clonación de una tarjeta, sin embargo, las formas de clonación más comunes son las siguientes: [32]

a) Clonación para compras: con esta modalidad se trata de copiar o duplicar la información incluida en la banda magnética de una tarjeta, para posteriormente incluirla en un plástico en blanco y a través de este segundo plástico hacer compras cuyo saldo se verá reflejado en el estado de cuentas del propietario de la tarjeta.

b) Clonación para retiros de cajeros: inicia con la reproducción de la información de la tarjeta; necesita, además, la adquisición de las claves o códigos de acceso del cliente para poder realizar retiros, puesto que como es sabido, sin esta clave o pin, no será posible hacer retiros de dinero en efectivo desde los cajeros automáticos, que es lo que se persigue con este hecho específico.

2.2.1 Tipificación: aplicación de la Ley 53-07, sobre Crímenes y Delitos de Alta Tecnología en la Republica Dominicana

En lo que respecta a la República Dominicana la clonación está penada en la Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología y se ubica en la clasificación de los crímenes y delito contra la confidencialidad, integridad y disponibilidad de datos y sistemas de información y en la misma se define la clonación como "la duplicación o reproducción exacta de una serie electrónica, un número o sistema de identificación de un dispositivo o un medio de acceso a un servicio"[33].

La ley anteriormente mencionada en su artículo 5 sanciona y castiga a los "Códigos de Acceso" como "el hecho de divulgar, generar, copiar, grabar, capturar,

[31] JARAMILLO ACEVEDO, Mariela. & ZAMBRANO, María. Migración de banda magnética a chip para evitar fraudes de clonación de tarjetas de crédito o débito. ¿los bancos ecuatorianos están preparados para este cambio? Guayaquil, Ecuador, 2013, p. 56

[32] Ob. Cit., p. 53

[33] REPÚBLICA DOMINICANA. Congreso de la Republica Dominicana. Sobre Crímenes y Delitos de Alta Tecnología [en línea]. Ley n.º 53-07 de 23 de abril de 2007 [consultado el 10 de enero de 2022]. Disponible en: https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf

utilizar, alterar, traficar, desencriptar, decodificar o de cualquier modo descifrar los códigos de acceso, información o mecanismos similares, por medio de los cuales se puede tener acceso de manera ilícita a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus elementos, o falsificar cualquier tipo de dispositivo de acceso al mismo, siendo la pena a imponer de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo"[34].

En el artículo se establece de la misma manera acerca de la "Clonación de Dispositivos de acceso" e indica que "la clonación, para la venta, distribución o cualquier otra utilización de un dispositivo de acceso a un servicio o sistema informático, electrónico o de telecomunicaciones, mediante el copiado o transferencia, de un dispositivo a otro similar, de los códigos de identificación, serie electrónica u otro elemento de identificación y/o acceso al servicio, que permita la operación paralela de un servicio legítimamente contratado o la realización de transacciones financieras fraudulentas en detrimento del usuario autorizado del servicio, se castigará con la pena de uno a diez años de prisión y multa de dos a quinientas veces el salario mínimo"[35].

La clonación de tarjetas en la República Dominicana es una praxis muy común que perjudica a muchas personas. Con esta práctica el delincuente persigue poder acceder a los recursos económicos de la víctima y provocar en el tarjetahabiente no solo un perjuicio económico sino también moral, asimismo provoca daños a la entidad financiera y pérdida de credibilidad por parte de usuarios. En ese sentido, hay que ser insistentes y reiterativos sobre los riesgos en que se incurre al utilizar este medio de pago y no tener en cuenta ciertos cuidados que se hacen imprescindibles tener al momento de utilizar la tarjeta en los diversos puntos de compra y venta.

Sin embargo, a pesar de las tantas denuncias, no son tantos los procesos que se judicializan y mucho menos los que obtienen condenas. Esto se debe a las dificultades de persecución ya que, en muchas ocasiones estas operaciones se llevan a cabo desde otros países y también porque en muchos casos las víctimas desisten, y al ser estos delitos públicos a instancias privadas no le queda otra opción al ministerio público más que retirar su acusación.

[34] Ob. Cit.
[35] Ob. Cit

2.3 Los diferentes métodos para clonar tarjetas

La clonación de tarjeta suele perpetrarse mediante el uso de dispositivos como el skimmer, minicámaras, falsos teclados, entre otros; los cuales permiten que los delincuentes obtengan informaciones o datos que les permita copiar la tarjeta original y, a partir de ahí y con los datos obtenidos (como claves personales), podrán utilizar el dinero del tarjetahabiente, ya sea utilizando el dinero o haciendo compras, como es lo más común, o simplemente para lo que ellos deseen. El método más habitual de clonación de tarjeta es denominado como skimming, es más, es común encontrar artículos en donde la clonación de tarjetas la denominan como skimming cuando existen otras modalidades que también se utilizan para clonar tarjetas.

El skimming es el método que se utiliza específicamente para clonar tarjetas con bandas magnéticas, se efectúa mediante un aparato que permite reproducir o duplicar la información incluida en las bandas magnéticas de las tarjetas sencillamente con deslizar el plástico a través de él. Carlos Cortez expresa que: "para este tipo de robo, el dispositivo utilizado es un "skimmer", un aditamento que se inserta en la ranura para la tarjeta en el cajero, el cual tiene una cámara para captar en video que cuando se teclea la clave, la graba instantáneamente y que, además, al deslizar la tarjeta al interior, se captura la información de la banda magnética[36].

Es decir, el hecho se perpetúa a tarjetas donde su diseño está basado en bandas magnéticas y su objetivo es capturar y realizar transacciones de pago no autorizadas por medio de un artilugio conocido como skimmer, el cual funge como el duplicador de la tarjeta, por medio de este se tiene como resultado una clonación tipo skimming.

El skimming se puede ejecutar de diversas maneras y en diversos lugares, la manera más simple que se puede dar es un restaurante o en una bomba de expendio de combustible, entre otros, donde solo basta con pasar la tarjeta por un skimmer y en cuestiones de segundos la tarjeta es clonada. Al realizar la clonación de esta manera, el estafador se limita a realizar consumos, sin acceso a poder extraer dinero de cajeros, pues requiere del pin de seguridad el cual en ese momento no tendría en su poder.

[36] CORTEZ, Carlos. Delito fácil y barato. El Mañana [en línea]. 26 de noviembre de 2012 [consultado el 8 de marzo de 2022]. Disponible en: https://www.elmanana.com/delito-facil-y-barato/1860062

La creatividad a la hora de clonar sube de nivel, cuando el estafador desea sustraer dinero de los cajeros automáticos pués, aparte de implantar un skimmer en el lector del cajero, estos delincuentes tecnológicos se apoyan en la instalación de microcámaras para captar el momento en que se introduce el pin de seguridad, logrando así una clonación completa. El proceso finaliza con la impresión de una nueva tarjeta a la cual se le graba toda la información sustraída.

Con la intención de reducir las clonaciones de tarjetas, las entidades financieras procedieron a agregar una mayor seguridad a las tarjetas adicionándoles un chip que en vez de almacenar la información procede a transferirla y dicha transferencia se realiza de manera encriptada y con esto se perdieron los skimmers su apogeo.

Sin embargo, paralelamente a la evolución de las tarjetas con bandas magnéticas a las de chip, evoluciona el skimming y surge el shimming, el cual se fundamenta en la clonación de la información de las tarjetas de crédito o débito en las que su diseño incluye un chip de seguridad. Para poder realizar el proceso de shimming, el perpetrador debe introducir en la ranura del dispositivo donde se vaya a introducir el chip de la tarjeta, una herramienta electrónica la cual es conocida como *shim.* El *shim* se compone de un microchip para decodificar y sustraer la información y una memoria de almacenamiento donde se guardan dichos datos.

Luego el estafador procede a recoger el *shim* e imprime los datos en una nueva tarjeta de banda magnética. El proceso para la obtención del pin de seguridad es igual que en la clonación tipo skimming.

Otra forma de clonar datos bancarios es a través del *phishing:* término que procede de la palabra inglés *fishing* que traducido al español significa pescar. Es decir, a través del *phishing* se lanza un anzuelo a los usuarios de la red cuya intención es pescar o atrapar a alguno para que revelen datos vulnerables.

El *phishing* puede ser conceptualizado como un fraude informático que tiene como objeto robar los datos personales de un usuario, tales como: contraseñas o claves para acceder a los servicios de la banca electrónica o por internet, número de tarjeta crédito a través de la suplantación de estas páginas bancarias o cualquier otra empresa.

Este fraude electrónico se lleva a cabo a través del envío de correos electrónicos que en principio dan la impresión de que proceden realmente de las entidades bancarias y financieras, y mediante este se le solicita "al usuario conectarse por medio de un enlace a un sitio web, el cual aparenta ser de alguna de las entidades anteriormente señaladas, generalmente por medio de una página pop-up que se abre por el mismo enlace, donde, al momento en que se ingresan los datos, estos son obtenidos por los defraudadores"[37].

Asimismo, el término ha sido utilizado como el proceso por el cual a una persona se le envía un correo, un mensaje o una llamada, que aparenta ser de una entidad bancaria legítima, para que introduzca sus datos personales, obtener asi las claves y otros datos. La víctima, pensando que verdaderamente se trata de un correo enviado por la entidad, proporciona estas informaciones privadas como su contraseña o datos de las tarjetas bancarias, sin percatarse de lo que está siendo víctima. "luego esta información obtenida de forma fraudulenta es utilizada por los ciberdelincuentes para acceder a las cuentas personales de las víctimas y causar pérdidas económicas o suplantación de identidad"[38].

Del *phishing* se desprenden varias modalidades, entre ellas las más conocidas son: el *smishing*: que es un tipo de *phishing* que se lleva a cabo, no mediante el envío de correos para suplantación de páginas web, sino, que se hace a través de teléfonos móviles vía mini mensajes de textos (SMS) o de cualquier aplicación de mensajería como WhatsApp. La otra manera se lleva a cabo mediante llamadas telefónicas en la que el impostor se hace pasar por empleado de la institución bancaria y busca obtener datos crediticios sobre la víctima; esta ha sido denominada como: *vishing.*

En ese orden, otro dispositivo electrónico fraudulento que se coloca en los cajeros automáticos con el fin de obtener información de las tarjetas originales cuando son introducidas por el cliente en el cajero y así ejecutar la acción fraudulenta, es el denominado facia. La facia, según se establece en declaraciones de testigos recogidas en la Sentencia penal núm. 371-06-2018-SSEN-00156 emitida por el Cuarto Tribunal

[37] CAMACHO CASTILLO, Miguel Angel. Solución de estrategia empresarial dominios de nivel superior para mitigar el fraude electrónico (PHISHING) en la banca electrónica por internet, Mexico, 2016.
[38] MARIANA LEGUIZAMÓN, Mayra Sheyla. EL PHISHING. Tesis de grado, Universitat Jaume. [sin fecha] [consultado el 3 de marzo de 2021]. P. 10. Disponible en: https://docplayer.es/5875905-El-phishing-trabajo-final-de-grado-grado-en-criminologia-y-seguridad-alumno-mayra-sheila-mariana-leguizamon-tutor-manuel-mollar-villanueva.html

Colegiado del Juzgado de Primera Instancia de Santiago, Distrito Judicial de Santiago, de fecha dos (02) del mes de agosto del año dos mil dieciocho (2018), es una metodología de fraude, que logra visualizar las informaciones de las tarjetas, informaciones que se quedan registradas en dichos dispositivos.

Siguen agregando estos testigos, que cuando se da la clonación por facia o lo que es lo mismo por la colocación de este dispositivo, el cajero emite una alerta al banco, puesto que se detecta que está siendo utilizada la tarjeta; esto permite que puedan tomarse las medidas de seguridad pertinentes para detener el fraude, como lo es por ejemplo la cancelación de la tarjeta que ha sido clonada al cliente. Cuando son colocados estos dispositivos las personas que lo hacen quedan identificadas en las cámaras de seguridad colocadas en los cajeros, las cuales abarcan distintos ángulos; establecen también que es un dispositivo de fácil instalación y que instalarla toma apenas unos cinco minutos.

Otra forma de clonar tarjetas es mediante el *trashing*: por medio de esta los estafadores van en busca de los váuchers de las tarjetas de crédito, que los tarjetahabientes botan después de haber hecho algún pago con sus tarjetas. Con estos comprobantes consiguen informaciones de las tarjetas y que luego son utilizadas indebidamente.

También está el *sniffing;* esta práctica de clonación de tarjetas se lleva a cabo a raíz de las transacciones realizadas a través de la web, y consisten en la intercepción de datos de pagos realizados en línea a través de tarjetas bancarias. Posteriormente se utilizan estos datos para consumar compras sin que el titular de la tarjeta se dé cuenta.

Finalmente, el *boxing,* el cual se da cuando al momento de los bancos enviar las tarjetas de crédito a las casillas de correo de sus titulares, mediante la utilización de sistemas informáticos y electrónicos, se interceptan los códigos de tarjetas de crédito necesarios para obtener datos de la tarjeta. Al violentar estos sistemas, los estafadores pueden acceder y obtener la información privada de estos clientes, y es así como luego pueden realizar transferencias de dinero hacia diferentes cuentas y de diferentes entidades bancarias con el fin de no ser rastreados.

2.4 Derechos y libertades afectadas: bienes jurídicos protegidos

Para estar ante la existencia de un delito, es imprescindible que, además de que exista un autor y una víctima, exista al mismo tiempo, un objeto sobre el cual recaiga la acción delictiva y un bien jurídicamente tutelado, es decir, un interés protegido.

La evolución casi incesante de los ciberdelitos, así como su impacto a nivel social, afecta tanto a personas físicas como jurídicas, soportando como consecuencia considerables daños patrimoniales mediante la afectación de sus bienes económicos y de su información personal, aquella que obtienen de forma ilegal los ciberdelincuentes. Sin embargo, antes de empezar a descifrar respecto a la protección del bien jurídico que se violenta o afecta a través de los delitos cibernéticos, específicamente respecto al ciberdelito de clonación de tarjetas, el primer término que debe ser definido es el de bien jurídico.

En ese sentido, y citado por Giovanni Grisales Pérez, Santiago Mir define en su texto el *Derecho penal general*, al bien jurídico como el "objeto de tutela jurídica"[39]; poniendo como ejemplo la vida, la intimidad, el honor, la propiedad, entre otros. A dichos bienes jurídicos, la ley penal los protege y castiga los ataques que surjan en contra de estos. Así, por ejemplo, el bien jurídico protegido en el caso de homicidio lo es la vida, pero en el de robo o estafa lo es el patrimonio económico.

Establecido lo anterior, la clonación de tarjeta afecta a las víctimas no solamente en lo que respecta a lo económico, sino también en lo laboral y emocional, puesto que en diversas ocasiones el dinero robado está reservado para cubrir sus necesidades esenciales, como gastos alimenticios, médicos, o para cumplir con sus obligaciones y realizar pagos de servicios básicos como luz o agua, entre otros.

En esa tesitura, en la Sentencia penal núm. 371-03-2019-SSEN-00166 de fecha diecisiete (17) del mes de julio del año dos mil diecinueve (2019), y emitida por El Primer Tribunal Colegiado del Juzgado de Primera Instancia de Santiago del Distrito

[39] GRISALES PÉREZ, Giovanni. Análisis dogmático de las conductas de Hurto por medios informáticos y semejantes (Art. 269i) y Transferencia no consentida de activos (Art. 269j) Ley 1273 de 2009. 2013. Universidad EAFIT. Maestría en Derecho Penal. [consultado el 8 de marzo de 2021]. P. 6. Disponible en: https://repository.eafit.edu.co/bitstream/handle/10784/1285/GrisalesPerez_GiovanniSaltin_2013.pdf;jsessionid=571C398EF368860555CC7EAB75C67E29?sequence=1

Judicial de Santiago, yacen las declaraciones de Juan Aníbal Rodríguez Fernández, víctima, quien en calidad de testigo, declaró en síntesis: …"Vengo a declarar en relación a un proceso penal que incoamos a raíz de que mi cuenta bancaria fue jaqueada y me robaron doscientos mil y picos de pesos, la cuenta es del Banco de Reservas, …; recibí un perjuicio porque esa era mi cuenta de nómina, ni la tarjeta pude pagar y tuve que pagar intereses por mora, además, había una parte de ese dinero que yo había ahorrado para solventar los gastos de mi hija que está estudiando en Barcelona, además no pude pagar los servicios de la casa, tuve que acudir a familiares que me facilitaran dinero para poder solventar los gastos de ese mes".

Partiendo de estas declaraciones se puede notar que, además de verse violentado la dignidad y la intimidad de esa víctima, como derechos que pueden ser vulnerados por los medios tecnológicos, también se pueden seguir nombrando otros tales como, el derecho patrimonial y la seguridad del estado, entre otros bienes tutelados por la ley constitucional dominicana.

Actualmente en el ordenamiento jurídico dominicano, la tutela y protección penal del bien jurídico de la intimidad se toma en cuenta desde varias esferas haciendo alusión a diversos elementos como son:

1) Los ataques tradicionales.
2) Las violaciones que suponen los nuevos sistemas de tecnologías de la información y la comunicación: control audiovisual clandestino, interceptación de todo tipo de comunicaciones, accesos ilícitos a datos y sistemas informáticos.

Tanto los instrumentos internacionales como la doctrina coinciden en indicar que las esferas de protección que caen dentro de la tutela del derecho a la intimidad y el honor personal comprenden: el secreto de los actos de la vida privada, la inviolabilidad de domicilio, el honor y dignidad de las personas, así como la inviolabilidad de secreto profesional y de las comunicaciones. Estos derechos componen aquellos conocidos como inherentes a la autonomía privada de las personas, y que ameritan su análisis individual para comprender como tal el bien jurídico o el derecho a la intimidad.

María Isabel Garrido Gómez expresa que, actualmente, en "la llamada sociedad de la información, adquiere gran relieve el reconocimiento y la garantía del derecho a la intimidad. Este derecho tiene una honda raigambre, pero es en la actualidad cuando ha adquirido una nueva comprensión, siendo uno de los derechos más vulnerados"[40]. Lo anterior da lugar a que la sociedad demande la salvaguarda de la información personal de cara a los posibles ataques mediante ciberdelitos.

Con el avance de las nuevas tecnologías y el posicionamiento de las redes sociales el robo de datos constituye uno de los ilícitos informáticos que afectan el derecho a la intimidad particularmente ahora como herramienta de comunicación. El robo de datos tiene dos móviles: poder acceder a los recursos económicos de la víctima o difamar y dañar la reputación de una persona y; también para crear un perfil en cualquier red social haciéndose pasar por esa persona, para perpetrar el delito mediante el phishing; estos aspectos se redimensionan ante la denominada sociedad de la comunicación, abogando por nuevos y suficientes mecanismos de protección ante los nuevos desafíos que traen consigo la tecnología de la información y la comunicación.

La tutela de la intimidad responde a varios factores, a saber:

1) El avance tecnológico que ha hecho necesario nuevas formas de incriminación y control ante las evidentes nuevas y sofisticadas conductas, tales como las estafas o fraudes informáticos realizados sobre los datos personales del individuo.

2) La influencia de la cultura anglosajona sobre el derecho a la *privacy*, el cual impacta en el desarrollo de la jurisprudencia y la doctrina respecto al derecho a la intimidad.

Por su parte, Jijena, manifiesta que "frente a las tecnologías de la información y comunicación la regla es que este derecho a la intimidad no se define, sino que se declara, pero que, en todo caso, sea concibiéndola ampliamente, sea declarándola, lo importante es que debe ser reconocida y tutelada"[41].

[40] BAUTISTA, Félix. La expresión y la intimidad. listindiario.com [en línea]. 2 de mayo de 2012 [consultado el 28 de mayo de 2022]. Disponible en: https://listindiario.com/puntos-de-vista/2012/05/02/230920/la-expresion-y-la-intimidad

[41] JIJENA, Renato**.** Chile, la protección penal de la intimidad y el delito informático. Editorial Jurídica de Chile. 1ª Edición, 1992. p. 42

Este delito no solo tiene afectación a los usuarios víctimas sino también a las entidades bancarias o emisores de tarjeta, y las consecuencias ante un fraude con tarjetas bancarias solo se podrán cuantificar con cifras que indiquen el importe total con el que ha sido defraudado el banco que emitió la tarjeta. Estos resultados, traen como consecuencia aspectos negativos que repercuten sobre el deterioro de la imagen de la entidad, la pérdida de credibilidad y como consecuencia, la pérdida en la cartera de clientes del banco, ya que algunos clientes optan por cancelar su producto tan pronto como saben que fueron víctima de robo.

2.4.1 La afectación al derecho a la protección del patrimonio

Hablando de derechos y libertades, la clonación de tarjetas representa una grave molestia tanto para la persona víctima del robo, así como también para las entidades bancarias y el sistema económico nacional como internacional, provocando grandes pérdidas patrimoniales mediante el robo de sus bienes económicos y datos e informaciones privadas a las cuales acceden los ciberdelincuentes sin ningún tipo de autorización, realizando diversos tipos de ataques a través de operaciones fraudulentas.

A partir de que se popularizara el uso del internet y de las tecnologías de la información y de la comunicación en sentido general, prontamente se reconocieron dos prototipos de peligros o inseguridades para los internautas. El primer peligro está vinculado a la intromisión en la vida privada de las personas, es decir, violación a la intimidad, tema que ya fue desglosado. El segundo peligro se relaciona con la integridad patrimonial, es decir, la afectación de los bienes, en este caso bienes económicos y financieros de los usuarios.

Las tarjetas bancarias, tanto de débito como de crédito, se han convertido en el primer eje de atención ante ataques no forzosos en contra del patrimonio de personas naturales como jurídicas, en razón del constante uso de tecnologías de la información y la comunicación al que nos vemos sujetos en la actualidad. Y, aunque haya otros fraudes que afectan al patrimonio, el cometido a las tarjetas bancarias sigue siendo el número uno. Es decir, ya no se está en presencia de un robo tradicional en el que se

hacía necesario tener que usar la fuerza y constreñir a la víctima para despojarla de sus bienes, ahora todo se vuelve tan fácil como dar un clic y clonar la tarjeta.

Siendo así, se debe tener en cuenta que, en el supuesto de la clonación de tarjetas bancarias, se genera un grave perjuicio, tanto a las víctimas que no pueden utilizarla mientras se encuentre suspendida, como al banco que se ve precisado a responder al cliente por las sumas que le han sido retiradas de manera fraudulenta. Asimismo, se afecta la economía de los estados ya que los bancos son parte del sustento de cualquier país.

Grisales entiende que "conductas como el hurto (robo) por medios informáticos y la transferencia no consentida de activos afectan tanto a personas naturales como jurídicas, padeciendo cada una de ellas graves detrimentos patrimoniales a través de la pérdida de sus bienes económicos e información privada a la que acceden de manera ilegal los delincuentes cibernéticos"[42].

Asimismo, otros autores como Franceso Carnelutti, consideran que estos comportamientos tienen como finalidad provocar un daño en el patrimonio del sujeto pasivo, es decir, la víctima, y que esta acción ilícita puede afectar directamente a la persona natural o jurídica o a su patrimonio económico.

En la República Dominicana, la jurisprudencia ha manifestado que el perjuicio o daño sufrido ante una acción de clonación de tarjeta "puede ser tanto moral como material. Y explica que será daño o perjuicio extrapatrimonial o no económico, el que resulta de los dolores, sentimientos, aflicciones, mortificaciones o privaciones y por contraposición, el daño material es aquel patrimonial o económico" (Suprema Corte de Justicia, septiembre del año 1961).

Al efecto, el Cuarto Tribunal Colegiado del Juzgado de Primera Instancia de Santiago del Distrito Judicial de Santiago, mediante Sentencia penal núm. 371-06-2018-

[42] GRISALES PÉREZ, Giovanni. Análisis dogmático de las conductas de Hurto por medios informáticos y semejantes (Art. 269i) y Transferencia no consentida de activos (Art. 269j) Ley 1273 de 2009. 2013. Universidad EAFIT. Maestría en Derecho Penal. [consultado el 8 de marzo de 2021]. P. 2 Disponible en: https://repository.eafit.edu.co/bitstream/handle/10784/1285/GrisalesPerez_GiovanniSaltin_2013.pdf;jsessionid=571C398EF368860555CC7EAB75C67E29?sequence=1

SSEN-00156, decidió emitir una sentencia a favor de la Asociación Cibao de Ahorros y Préstamos, querellante y actor civil, la cual se vio perjudicada con el ilícito penal ejecutado por el imputado Rainier Abreu Gómez, puesto que sufrió un daño material económico, por el deterioro de sus cajeros con la colocación de dispositivos fraudulentos, y los gastos en que incurrió en la reparación de los mismos.

Establecido lo anterior, para el caso de clonación de tarjetas, el bien jurídico que se afecta es el patrimonio económico no solo de las personas físicas sino también de las diferentes entidades bancarias; además de la protección de la información y de los datos privados de las personas o de sus bienes que reposen en registros tanto públicos como privados. Estos datos comprenden aquellos nombres, códigos, claves, números ya sea de tarjetas o cuentas bancarias o números de cédulas, que se requieren para que los ciberdelincuentes puedan acceder a los sistemas bancarios de las víctimas

2.5 Impacto de la pandemia por COVID-19 en el aumento del ciberdelito de clonación de tarjetas

La pandemia del COVID-19 ha sido uno de los más grandes retos a los que ha tenido que enfrentarse el mundo en los últimos años no solo por la crisis de salud y las pérdidas de vidas, sino también por la incertidumbre ante todo lo que ocurría y la crisis económica que se avecinaba.

En ese mismo sentido, en menos tiempo del imaginado, se aceleró el proceso de transformación digital que no se esperaba ocurriera tan rápido y es que, ante la necesidad de evitar el contagio, no hubo más opción que permanecer aislados. Ante tal situación, las personas se vieron obligadas a trabajar, estudiar y hasta socializar desde casa y como consecuencia, la tecnología y el internet se volvieron una herramienta de vital importancia resaltando hacia estos una dependencia como nunca antes.

La pandemia de la COVID-19 y el incremento de la actividad digital que ha generado en la región, ha dejado aún más en evidencia las vulnerabilidades del espacio digital de América Latina y el Caribe[43], es decir que, hay que destacar que, así como la

[43] Reporte de ciberseguridad 2020 riesgos y avances y el camino a seguir en América Latina y el Caribe. Disponible en Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe (iadb.org)

pandemia ha fortalecido la era de la digitalización, también ha fortificado a los cibercriminales, ya que estos se han aprovechado de las brechas en ciberseguridad existentes, lo que rápidamente ha contribuido a la comisión de más delitos cibernéticos.

Asimismo, el aumento del dinero y la bancarización digital dio lugar a un sinnúmero de ataques cibernéticos relacionados con tarjetas, cajeros y sistemas de pago; convirtiéndose la frecuencia de pagos en línea en uno los principales obstáculos de la economía digital ya que, estos se han traducido en un abanico de nuevas posibilidades para los delincuentes atraer la atención de los usuarios de dinero digital y así robarles sus datos personales y hacerse transferencias o consumos con sus tarjetas.

Durante la pandemia se cometieron muchas estafas y fraudes a cuentas bancarias; el método más habitual de fraude lo constituyó el *phishing*, el robo virtual, generado a través de un correo o mensaje relacionados al COVID-19 como anzuelo para solicitar actualización de credenciales, poder luego inmiscuirse en los diferentes sistemas de información y así proceder a robar claves de acceso a internet banking o de datos de tarjetas de crédito o débito y luego poder transferirse los fondos.

También están en auge los ataques a través de programas maliciosos (*malware*) como aquellos programas espías, ladrones de información o los troyanos bancarios.

En esa misma línea, fue publicado en el periódico Hoy, en fecha seis (06) de mayo de 2020 que la empresa Fortinet, (dedicada a al desarrollo de software y servicios de ciberseguridad, a través de su plataforma Fortinet Threat Intelligence Insider Latin America), "anunció los hallazgos del primer trimestre de 2020, manifestó que la región de América Latina y el Caribe, incluyendo República Dominicana, sufrió aproximadamente 3 millones de intentos de ataques de virus y malware en el primer trimestre del año por medio de amenazas de phishing"[44].

También, la empresa hizo mención de que "tan sólo durante marzo y coincidiendo con el confinamiento por la pandemia del COVID-19 en la mayoría de los países, se produjo un promedio de 600 nuevas campañas diarias de phishing a nivel

[44] Aumenta el cibercrimen en República Dominicana en el contexto de COVID-19. Hoy Digital [en línea]. 06 de mayo de 2020 [consultado el 8 de mayo de 2022]. Disponible en: https://hoy.com.do/aumenta-el-cibercrimen-en-republica-dominicana-en-el-contexto-de-covid-19/

mundial, una estafa digital que envía mensajes con enlaces maliciosos y lleva al usuario a divulgar datos personales y bancarios en páginas web falsas o a descargar virus que controlan los dispositivos y roban información"[45].

Asimismo, reportó que República Dominicana fue víctima de "más de 48 millones de intentos de ciberataques en el primer trimestre del año, sumando al total de 9,7 billones en América Latina y el Caribe[46]". Es decir, debe decirse que ante el contexto COVID-19 hubo un aumento de los ciberdelitos en República Dominicana, en especial en aquellos que inciden en el patrimonio económico de los ciudadanos y esto no solo es producto de la creatividad de los delincuentes ante tanto tiempo de ocio por el confinamiento sino también a la recesión económica.

Otra de las estafas más comunes que se detectaron durante la pandemia fueron las que se cometieron a través de llamadas telefónicas, cuyo único fin era el de engañar a las personas para así obtener los datos de sus cuentas bancarias. En cualquiera de los casos, la finalidad es la misma, robar credenciales, claves y otros datos confidenciales.

Según el informe Global Cybersecurity Outlook elaborado por El Foro Económico Mundial, el cual se encarga de destacar las tendencias y evaluar los desafíos sobre ciberseguridad: "la cantidad de ataques cibernéticos por organización aumentó un 31 % en 2021 en comparación con 2020. El precio de estas infracciones también se ha disparado, y las organizaciones necesitan un promedio de 280 días para detectar y responder a un ataque cibernético. Además, en 2021, cada ciberataque exitoso podría haberle costado a una empresa alrededor de $ 3.6 millones. Por lo tanto, los ataques cibernéticos son un problema importante que afectará a alrededor del 55 % de las empresas de todo el mundo en 2021"[47].

Por otra parte, y para puntualizar algunos casos de defraudaciones de tarjetas que hemos tenido en nuestro país, hay que hacer mención que en el devenir de los años en la Republica Dominicana han existido una serie de programas de ayuda económica a familias de escasos recursos; el primero de ellos es el conocido programa Progresando

[45] *Ibidem*
[46] *Ibidem*
[47] ATHAL, Krishna. La correlación entre Covid-19 y el ciberdelito. Entrepreneur [en línea]. 22 de marzo de 10 [consultado el 8 de mayo de 2022]. Disponible en: https://www.entrepreneur.com/article/421994

con Solidaridad que bajo el gobierno de Luis Abinader, pasó a llamarse Supérate. Mediante estos programas, el gobierno otorga a cada familia una tarjeta prepaga que permite hacer compras a su titular en determinados establecimientos. Asimismo, permite manejar varios subsidios al mismo tiempo, como lo referente al bono luz y al bono gas.

Estas tarjetas o programas se volvieron muy populares luego de que llegara la Pandemia COVID-19 debido a que, muchas familias al no poder salir a las calles a trabajar, obtuvieron con estos programas (Quédate en casa, Pa´ ti, Tarjeta de Solidaridad) su única forma de adquirir alimentos y cubrir otras necesidades básicas imprescindibles para subsistir. Sin embargo, miles de dominicanos que fueron favorecidos con estos programas o que les fue otorgada la Tarjeta Supérate (antigua tarjeta de Solidaridad), fueron víctimas de suplantación o clonación de sus datos y tarjetas y no pudieron hacer uso de sus ayudas.

En ese tenor, y tomando como referencia uno de los casos ocurridos en Santiago, se le impuso a varios ciudadanos, como medida de coerción, el cumplimiento de tres meses de prisión preventiva, luego de haber sido desmantelada una banda que se dedicaba a la clonación de tarjetas de la Administradora de Subsidios Sociales (ADESS) (Tarjetas de Solidaridad), en perjuicio del Estado dominicano y cuyos daños se perciben por más de un millón y medio de pesos. Este caso, además, el tribunal lo declaró complejo, ya que los acusados perpetraban muchas de sus acciones desde diferentes ciudades del país.

En este caso, hay que mencionar que uno de los imputados era empleado del ADESS y elaboró en conjunto con los demás implicados una estrategia a través de la cual duplicaban las informaciones electrónicas que se encontraban en las bandas magnéticas de las tarjetas para luego realizar transacciones fraudulentas, tanto con tarjetas clonadas como auténticas (pero de las cuales tampoco eran propietarios), en los diferentes negocios adheridos a la Red de Abastecimiento Social (RAS), que cambiaban por dinero en efectivo, el cual posteriormente se lo distribuían a su favor. Es decir, que se estaban lucrando con los fondos públicos que el Estado depositaba a los favorecidos de las tarjetas Progresando con Solidaridad.

La Administradora de Subsidios Sociales (ADESS) fue quien se encargó de hacer la denuncia y de acuerdo a los hechos, a los implicados se les acusa de los delitos de uso de documentos falsos, asociación de malhechores, estafa contra el Estado dominicano y abuso de confianza, tipificados en los artículos 148, 265, 266, 386 y 405 del Código Penal Dominicano; también de violar los artículos 5, 14 y 17 de la Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología, concernientes a clonación de tarjetas (códigos de acceso), obtención ilícita de fondos y robo de identidad.

Otra modalidad de clonación de tarjetas que se ha incrementado en nuestro país, es el conocido en los barrios como “chipeo/ shipeo” o "tarjeteo". El chipeo/shipeo o tarjeteo es la nueva tendencia de estafa cibernética que está envolviendo a la República Dominicana. Este “oficio” bastante productivo, pero ilícito, consiste en la compra de datos privados de personas de cualquier parte del mundo, especialmente de residentes en los Estados Unidos, que previamente han sido víctimas de robo de datos personales y/o crediticios, para luego hacer uso de los recursos económicos de esas personas. Otra forma de chipeo también puede darse a través de llamadas telefónicas.

Por lo general, estos datos se adquieren en páginas de internet que se dedican a suplantar páginas, en este caso, páginas bancarias, para luego vender estos paquetes de información personal y crediticia, los cuales suelen pagarse a través de moneda virtual. Posteriormente realizan compras, por lo general, fuera del país, cuyo importe le es cargado al propietario de la cuenta; luego, esos objetos comprados son recogidos por una persona que consecutivamente las envía a territorio dominicano; de esto es que surge que algunas personas entiendan que el término ´´shipeo´´ proviene de la palabra inglesa *shipping*: que no es más que el envío o traslado físico a través de un transportista de una mercancía desde un lugar hasta otro, hasta llegar al cliente.

De esto se puede colegir, que para llevar a cabo este fraude se necesita de todo un entramado, de manera que se trata de una red de operaciones que realizan más de una persona tanto en territorio nacional como internacional, en donde cada una de ellas cumple con un rol particular.

El esquema de negocio de los tarjeteros o chiperos, como se denominan aquellos a los que se dedican a este oficio, envuelve tantos beneficios económicos que es muy

fácil identificarlos ya que, sin mucho precedente cambian su forma de vestir, se hacen notorios los lujos, las prendas de oro, los vehículos de alta gama, la adquisición de propiedades costosas y el estilo de vida desenfrenado, haciéndose visible que presumiblemente detrás de ellos haya algún negocio ilícito.

Continuando por la línea de los vehículos, vale recordar que hubo una época en la que los carros Honda Civic modernos, se asociaban a que sus conductores o propietarios eran personas que se dedicaban al chipeo o tarjeteo en el país; y muchos ciudadanos se molestaban cuando miembros de la Policía Nacional les solicitaban detenerse, al ser catalogados o confundidos como chiperos solo por andar en uno de estos vehículos.

En la actualidad, muchos jóvenes entran al mundo del chipeo o tarjeteo, ya que entienden que es un negocio que les deja muchos beneficios económicos sin tener que poner su vida en riesgo, pero sí su libertad. Esto en razón de que, por las incidencias que tienen estas conductas, acarrean graves resultados, ya que, por el modus operandi bajo el cual actúan, se violan leyes tanto de territorio nacional como internacional por lo que se empeoran las consecuencias.

Capítulo III. Política criminal del ciberdelito de clonación de tarjetas en la República Dominicana

En el siguiente y último capítulo se ofrecen informaciones acerca de la política criminal llevada a cabo en la persecución del ciberdelito de clonación de tarjeta. En este se encuentra cuáles son las entidades encargadas de la persecución, qué dificultades se presentan con relación al manejo de la prueba, las problemáticas en la persecución debido al carácter transnacional de este tipo de delitos y la colaboración que se deben dar los países. Además, cómo se ha desarrollado el tema de la ciberseguridad en la República Dominicana.

3.1 Entidades encargadas de la persecución del ciberdelito

La ley 53-07, describe en su contenido cuales son los organismos competentes creados a fin de perseguir los ciberdelitos. En ese contexto, la Policía Nacional a través del Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) en

conjunto con el Ministerio Público (y su dependencia especializada) son las principales entidades facultadas de llevar a cabo cualquier proceso de investigación de delitos cibernéticos, procurando de esta manera asegurar mejores resultados cuando concluya la investigación. Así mismo, la División de Investigación de Delitos Cibernéticos (DIDI) como dependencia del Departamento Nacional de Investigaciones (DNI). Mientras que, para el diseño de la política criminal creó la Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología (CICDAT).

Para comenzar a puntualizar, el Ministerio Público el 4 de febrero del 2013, creó su dependencia especializada para tratar delitos de alta tecnología y es la que se conoce como: Procuraduría Especializada contra el Delito de Alta Tecnología (PEDATEC). El PEDATEC es una entidad "compuesta por fiscales, abogados, informáticos y peritos dedicados a trabajar los delitos que se cometen a través de cualquier dispositivo tecnológico, amenazas vía telefónica, clonación de tarjetas, difamación a través de las redes sociales, obtención ilícita de fondos, transferencia electrónica ilícitas de fondos, estafa electrónica, chantaje vía telefónica, robo de identidad, adquisición y posesión de pornografía infantil online"[48].

Su función principal es regular, concientizar y aplicar la Ley 53-07, sobre Crímenes y Delitos de Alta Tecnología, debiendo sentar las bases respecto a una efectiva investigación, persecución y represión contra este tipo de crímenes. Asimismo, deben asesorar a otras fiscalías en lo que se refiere a acciones penales que deban ser iniciadas y así asegurar que los procesos se agilicen preservando con esto los derechos de los ciudadanos víctimas de algún ciberdelito, tal como queda establecido en las leyes.

De la misma forma, investigar y someter los delitos sobre apropiación indebida (estafa electrónica, clonación de tarjetas, obtención ilícita de fondos, transferencias ilícitas, comercio ilícito de bienes y servicios en medios electrónicos, código malicioso, apropiamiento de páginas web, dominios, etc., piratería); delitos de suplantación de identidad (robo de identidad, falsificación de documentos y firmas, difamación a través

[48] SANTOS LORENZO, Maritza. *Análisis de los medios probatorios idóneos para comprobar los delitos electrónicos en el Distrito Nacional, año 2019*. En: https://bibliotecaunapec.blob.core.windows.net/tesis/TPG_CI_MDP_06_2020_ET210180.pdf [base de datos en línea] [consultado el 15 de mayo de 2022]. Tesis de postgrado, Universidad APEC, 2020. P. 49. Disponible en: https://bibliotecaunapec.blob.core.windows.net/tesis/TPG_CI_MDP_06_2020_ET210180.pdf

de las redes sociales, chantaje vía electrónica, amenazas vía telefónica); y, delitos sexuales a través del Internet (distribución de material sexual con fines maliciosos, atentados sexuales, elaboración, venta y distribución de pornografía infantil, adquisición y posesión de pornografía infantil[49].

Como dependencia de la Policía Nacional, está el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT), cuyas funciones principales, según la Ley 53-07, son: "velar por el fiel cumplimiento y ejecución de las disposiciones de la Ley 53-07, investigar todas las denuncias de crímenes o delitos considerados de alta tecnología, responder con capacidad investigativa a todas las amenazas y ataques a la infraestructura crítica nacional, desarrollar análisis estratégicos de amenazas informáticas y, velar por el correcto ordenamiento del personal de la unidad de investigación"[50].

Siguiendo esa línea, el DICAT debe trabajar en combinación con: 1) la Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología (CICDAT), (comisión también creada por la ley 53-07 y de la cual se hará mención más adelante); 2) la Red Internacional 24/7 que se encargará de asistir en "Crímenes que Involucran Alta Tecnología perteneciente al Subgrupo de Crímenes de Alta Tecnología del Grupo de Expertos en Crimen Organizado Transnacional G8"[51]; y, 3) con cualquier otro organismo, ya sea nacional o internacional que por igual se encargue de investigar crímenes y delitos tecnológicos.

Es oportuno decir que el personal que conforma el DICAT, debe poseer vastos conocimientos y experticia en áreas especializadas de la informática y/o ciencias afines, así como también en procesos de investigación. El comandante que dirija el departamento es inamovible y debe permanecer en su cargo por espacio de dos años mínimo, a menos que no demuestre tener las capacidades suficientes para cumplir con las funciones del puesto. Bajo estas circunstancias podrá ser destituido antes de cumplir con el mínimo del tiempo requerido en el cargo.

[49] Procuraduría Especializada Contra Crímenes y Delitos de Alta Tecnología. Procuraduría General de la República Dominicana [en línea]. [s.d] [consultado el 10 de mayo de 2022]. Disponible en: https://pgr.gob.do/pedatec/
[50] REPÚBLICA DOMINICANA. Congreso de la Republica Dominicana. Sobre Crímenes y Delitos de Alta Tecnología [en línea]. Ley n.º 53-07 de 23 de abril de 2007 [consultado el 10 de enero de 2022]. Disponible en: https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf
[51] Ibídem

Otro organismo cónsono a la función de perseguir e investigar delitos informáticos, y subordinado al Departamento Nacional de Investigaciones (DNI), es la División de Investigación de Delitos Informáticos (DIDI). Este organismo se encarga de responder las denuncias e investigar sobre los delitos y crímenes de alta tecnología que exclusivamente se cometen en contra de la humanidad, la Nación, el Estado, la seguridad nacional o que incluyan al presidente de la República o ministros en funciones. En otro ámbito, deben asimismo implementar procesos para el manejo y enfrentamiento de amenazas informáticas y fomentar el constante aprendizaje del personal que integra el departamento de investigación.

Al igual que como se le exige al personal que conforma el DICAT, todos los que conforman la DIDI deben tener las competencias y las aptitudes necesarias que acrediten sus conocimientos en las áreas afines a la informática y a la investigación. Así como también, trabajar en combinación con la CICDAT y cualquier otra entidad de investigación de crímenes y delitos tecnológicos tanto nacional como internacional.

Siguiendo la secuencia, se ha hecho mención de la Comisión Interinstitucional Contra Crímenes y Delitos de Alta Tecnología (CICDAT), delegación cuyo fin es similar a los establecidos en los organismos anteriores pero que, de manera específica se encarga, entre otras cosas, de coordinar, cooperar y promover tanto con las autoridades de investigación como judiciales, con gobiernos e instituciones nacionales y extranjeras, en la búsqueda de eficientizar, prevenir y reducir los niveles de delitos informáticos que sean cometidos en el territorio dominicano.

Esta comisión está compuesta por representantes de diferentes entidades locales, a saber: La Procuraduría General de la República, El Ministerio (antigua secretaría) de las Fuerzas Armadas, El Ministerio (antigua secretaría) de Interior y Policía, “La Policía Nacional, La Dirección Nacional de Control de Drogas (DNCD), El Departamento Nacional de Investigaciones (DNI), El Instituto Dominicano de las Telecomunicaciones (INDOTEL), La Superintendencia de Bancos de la República Dominicana, El Consejo Nacional para la Niñez y la Adolescencia (CONANI) y El

Instituto Tecnológico de las Américas (ITLA)"[52]; siendo la Procuraduría General de la República la que preside la comisión y, el Instituto Tecnológico de las Américas (ITLA) quien funge como secretario general y se encarga de convocar a reuniones, hacer públicas las decisiones que se tomen y capacitar a las autoridades competentes o cualquier otra que sea necesaria.

Cada una de estas instituciones, aúnan esfuerzos no solo para que se cumpla la ley y se desarrollen políticas de mejoras sino también para incentivar la admisión de cualquier convenio o tratado internacional que surja en la materia tendente a prevenir, perseguir y reducir la comisión de delitos informáticos.

3.1.1 Técnicas o procedimientos de investigación

El esquema de investigación del ciberdelito de clonación de tarjetas, lleva a prestar atención a cuestiones propias de este tipo de delitos. Una vez, el tarjetahabiente se ha dado cuenta que fue víctima de clonación de su tarjeta, el primer paso que debe dar es alertar a la institución bancaria a la que está afiliada su cuenta ya sea de débito o de crédito. La entidad bancaria procede a evaluar bajo qué circunstancias se dio "la clonación" para determinar cuál será su postura y si decide devolver o no la suma de dinero gastada a su propietario.

El segundo paso consiste en dar voz al departamento correspondiente. En ese tenor, en la ciudad de Santiago de los Caballeros, las infracciones sobre clonación de tarjetas son denunciadas en el Departamento de Falsificaciones y Delitos Especiales de la Fiscalía, allí la persona que recibe la denuncia conversa con el tarjetahabiente para poder identificar la manera en la que se vio comprometida su tarjeta, si se trató de una clonación a través de phishing o una de sus modalidades o si por el contrario se trató de una clonación física de la tarjeta; posteriormente, en conjunto con el DICAT se inicia la investigación; los policías y forenses analizan las evidencias a través de un programa electrónico llamado celery el cual produce un informe con las informaciones que se obtengan del dispositivo analizado; para los casos de clonación se extraen las

[52] REPÚBLICA DOMINICANA. Congreso de la Republica Dominicana. Sobre Crímenes y Delitos de Alta Tecnología [en línea]. Ley n.º 53-07 de 23 de abril de 2007 [consultado el 10 de enero de 2022]. Disponible en: https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf

informaciones de las tarjetas que han sido deslizadas por el skimmer (si esto es lo que se está analizando), acto seguido se le envía el informe concluido al Ministerio Público con cualquier otro elemento. El ministerio público solicita las autorizaciones necesarias para determinar los propietarios de las tarjetas clonadas o cualquier otra información o levantamiento que se requiera hacer y que sea necesaria para continuar con la investigación entiéndase, orden de arresto, allanamiento o cualquier otra.

Para el caso de clonación de tarjetas no presentes (aquellas que se dan a través del phishing o sus modalidades), el proceso de investigación se complica un poco más porque muchas veces las personas que se dedican a robar los datos bancarios de una persona, son miembros de grupos que operan desde las cárceles del país y que compran chips telefónicos desechables para realizar las llamadas haciéndose pasar por empleados del banco, lo que imposibilita el rastreo.

Como se ha dicho anteriormente, el delito de clonación de tarjeta es público a instancia privada, lo que quiere decir que la acción del ministerio público está sujeta a la denuncia que interponga la víctima y sin ella no puede ejercer ningún movimiento. La denuncia o la querella (en caso de que sepa quién es el imputado) es lo que lo apodera. Resulta también importante recordar, que, como todo proceso judicial, y más estos de ciberdelitos que son tan burocráticos, si no se cumplen las formalidades requeridas tanto por el Código Procesal Penal Dominicano como por la ley 53-07, contra Crímenes y Delitos de Alta Tecnología, para llevar a cabo la investigación, estos procesos no prosperarán y como consecuencia, habrá muchos casos que quedarán impunes.

Finalmente, dice Miguel Valdemar Díaz[53], que según estudios realizados en la República Dominicana, el país o las entidades encargadas de investigar estos delitos, cuentan con los recursos tecnológicos adecuados para enfrentar el ciberdelito, sin embargo, lo que se refleja en la realidad es otra, porque no en todas provincias se vislumbra tal avance. Y es que, para agregar a lo que indica Valdemar, no en todas las provincias existen departamentos especializados para trabajar de manera exclusiva con los ciberdelitos, además, tampoco el personal especializado es suficiente ni está debidamente capacitado.

[53] DIAZ VALDEMAR, Miguel. El ciberdelito una actividad rentable en la República Dominicana. *El Nuevo Diario (República Dominicana)* [en línea]. 18 de marzo de 2022 [consultado el 10 de mayo de 2022]. Disponible en: https://elnuevodiario.com.do/el-ciberdelito-una-actividad-rentable-en-la-republica-dominicana/

3.1.2 Manejo de evidencias: problemáticas

El uso de aparatos telemáticos o electrónicos, el internet y las posterior era de la digitalización ha traído notables cambios en los procedimientos para recolectar y preservar pruebas o evidencias que deban ser presentadas en un tribunal de justicia a fines de esclarecer sobre la comisión de ilícitos cibernéticos. Como resultado, se ha introducido una nueva categoría de evidencia: la evidencia electrónica o digital.

Ahora bien, en palabras de Santiago Acurio Del Pino, evidencia electrónica y digital corresponden a diferentes categorías y, cada una de ellas "hacen una necesaria distinción entre el elemento material de un sistema informático o hardware (evidencia electrónica) y la información contenida en este (evidencia digital). En este contexto el hardware se refiere a todos los componentes físicos de un sistema informático, mientras que la información, se refiere a todos los datos, programas almacenados y mensajes de datos trasmitidos usando el sistema informático)"[54]. Sigue agregando, además, que es útil hacer esta distinción porque en base a ello se podrán trazar procedimientos que vayan acorde a la evidencia de que se trata y se podrá diferenciar "una escena física del crimen y una digital"[55].

Por esta razón, se entiende que sería más práctico acuñar el término de evidencia digital porque es más sobre esta que recaen los cambios respecto a su manejo: entiéndase los procedimientos para su búsqueda, su obtención, su análisis, preservación y presentación la cual, ante toda circunstancia debe siempre basarse en principios tales como: la autenticidad, la fiabilidad, la exactitud.

Para comenzar a definirla, se puede decir que la evidencia digital es todo dato que esté almacenado o haya sido transmitido a través de tecnología informática y que será utilizada para establecer la hipótesis respecto a la comisión de un ciberdelito. En palabras más simples, es todo aquello que se encuentre guardado o registrado en un aparato telemático, informático o electrónico.

[54]del Pino, S. A. (2019). Manual de manejo de evidencias digitales y entornos informáticos. Versión 2.0.
[55] Ibidem.

La recolección y posterior presentación ante un tribunal, de una evidencia digital, debe considerarse tomando en cuenta el momento en el que esté el proceso de investigación del ciberdelito. En ese sentido, la primera etapa se relaciona con la recolección y el análisis que se le hacen a los aparatos telemáticos, informáticos o electrónicos para encontrar la evidencia digital. La segunda, tiene que ver con los procedimientos que tienen que llevarse a cabo para la presentación de estas evidencias ante un tribunal ya que, para su presentación se debe recurrir a tecnologías (instalación de instrumentos tales como pantallas, computadoras, cámaras, entre otros).

En ambos casos se presentan dificultades claras: en el primero, por la cantidad de datos que pueden ser encontrados en el dispositivo y todo los procesos que tienen que hacer los peritos para poder recolectar estos datos; en la segunda fase porque, a pesar de que el Consejo del Poder Judicial dominicano, a través de su programa visión justicia 20-24 se propuso digitalizar todos los procesos judiciales dominicanos, (programa que se adelantó ante la declaratoria de la pandemia por COVID-19 y que efectivamente transformó el acceso a la justicia hacia el uso de medios digitales) no menos cierto es que la instalación y mantenimiento de esos programas y equipos constituyen una considerable inversión económica para el sistema judicial y todavía hay tribunales que no cuentan con los medios, los recursos o el conocimiento. Además de, las fallas técnicas (eléctricas, red, conexión de los aparatos, entre otros) que con frecuencia se presentan en aquellos tribunales que si disponen de los medios.

Para seguir con el tema de las dificultades y, a pesar de que hay que reconocer que ha habido avances respecto a la atención que se le ha venido dando a la evidencia digital, es necesario hacer referencia a que siguen presentándose problemas y es que, ante la revolución o evolución de la era digital en donde casi todo se encuentra digitalizado, las herramientas (tanto en hardware como en software) utilizadas para eficientizar los procesos de investigación e identificación de evidencia digital no son suficientes para responder a la demanda lo que se convierte en un desafío para los peritos informáticos.

En otro orden, hay que tener pendiente que los datos digitales son muy sensibles y si no se tienen en cuentan medidas especiales estos pueden borrarse o modificarse tan sencillo como al apagar o desconectar el aparato. Esto se debe a que la información se

almacena en una memoria volátil, es decir, la información se guarda temporalmente y cada vez que se reinicia o apaga el dispositivo, la información se borra. Diferente a lo que ocurre con los dispositivos de almacenamiento no volátiles, ya que estos no necesitan estar conectados de forma continua para conservar a corto o largo plazo los datos contenidos en estos.

Asimismo, el delincuente a través de aplicaciones o programas de escritorio remoto, tales como AnyDesk, TeamViewer, entre otros, puede acceder al dispositivo e introducir cambios intencionalmente, hecho que dificultaría al final del levantamiento y presentación de evidencia, el conseguir una condena justa. Como fruto de esa debilidad, surge la necesidad de conservar la integridad de la prueba digital lo que, además, la convierte en un principio fundamental del manejo de las evidencias digitales. El principio de la integridad resulta ser imprescindible para garantizar la exactitud y fiabilidad de las pruebas digitales.

En ese sentido, el manejo de este tipo de evidencias requiere del uso de normas y procedimientos que procuren salvaguardar la pertinencia y utilidad de las mismas ya que son esenciales para el esclarecimiento de ciertos delitos. Esto abarca asuntos que pueden ir desde el empleo de tecnologías hasta la intervención del personal debidamente calificado para su manipulación. Esto quiere decir, que el reto no se circunscribe solamente a estar al tanto de cuáles son las últimas tendencias a nivel de tecnología, sino también a que los peritos informáticos requieren equipos que los pongan a nivel de dar respuestas acordes a la magnitud del problema en que les toque intervenir. En este punto, es importante señalar que al menos en la ciudad de Santiago de los Caballeros no existen los suficientes peritos para dar a basto, quizás no solo con el manejo de casos de clonación de tarjetas sino también con otras investigaciones de ciberdelitos que le correspondan hacer.

En sentido general, se debe tener en cuenta que para analizar o recuperar de un dispositivo informático cualquier material contenido en su almacenamiento, y que se presuma que pudiera ser indicio de un ciberdelito, debe ser manipulado con cuidado, ya que las evidencias digitales tienden a ser volátiles, frágiles, sensibles al momento de ser recuperadas, esto debido a que muchos datos pueden ser alterados, destruidos o borrados en tiempo real y/o de forma remota. Asimismo, las intervenciones para la

investigación y recuperación de estas evidencias deben ser consumadas por un técnico certificado en la materia, a los fines de que tomen en cuenta todos los pasos necesarios para que no se afecte la integridad de la evidencia ni tampoco de las personas involucradas en el proceso.

Tomando en cuenta los cuidados que hay que tener para recolectar y preservar una prueba digital, el proceso de levantamiento de las evidencias digitales puede establecerse de la siguiente manera:

1. Lo primero que procede es identificar la evidencia a ser recolectada.
2. Se realiza una fotografía panorámica del lugar para recrear la escena, en este caso sería del lugar y los aparatos o dispositivos involucrados.
3. Identificación de evidencias: si se trata de la adquisición de evidencia volátil no se deberá apagar ningún dispositivo que se encuentre encendido, ya que se perdería información.
4. Determinación de almacenamientos: en este caso, se procede a apagar y desconectar de las fuentes de electricidad de los dispositivos que estén prendidos. Es decir, apagar estos dispositivos para luego extraer las unidades de almacenamiento y finalmente, se le hacen fotos a fin de obtener una copia exacta y de resguardar la evidencia original.
5. Cadena de custodia: se debe registrar el manejo y almacenamiento que se da a cada una de las piezas que fueron recolectadas.
6. Preservación: en esta fase se resguarda la evidencia, se embalan y sellan la evidencia clasificando las mismas en función al tipo de evidencia.
7. Finalmente, se traslada la evidencia, se completa la cadena de custodia y se indican la fecha, hora de entrega, observaciones y las generales de quien envía y recibe.
8. Una vez concluidos los pasos anteriores, lo recolectado y analizado se envía a las autoridades correspondientes para que presenten su acto conclusivo.

En lo que respecta al proceso de levantamiento de las evidencias del delito de clonación de tarjetas, en los casos de clonación de tarjetas presentes (físicas), se da la ventaja de que los principales elementos que se recogen y que indican que se ha cometido la infracción, ya que en repetidas ocasiones las personas son arrestadas en flagrante delito, son las tarjetas de los bancos y los plásticos para tarjetas en blanco, y

como se deduce estas son evidencias físicas y por ende no persiste tanto el riesgo de pérdida, alteración u otro daño de los que sí son susceptibles las evidencias digitales. Es decir, que los elementos que se obtienen son físicos.

Ahora bien, el skimmer, que es el instrumento que se utiliza para obtener y posteriormente replicar los datos de las tarjetas, es un aparato electrónico que, en caso de serle ocupado al ciberdelincuente, sirve de evidencia digital del delito, ya que una vez el perito lo conecta a su programa de recuperación de información este puede extraer los datos de todas las tarjetas que han sido pasadas por ese dispositivo. Igual, además del skimmer, puede encontrarse cualquier computador al momento de allanar un "laboratorio" dedicado a la clonación.

En los casos de tarjetas no presentes, como en el caso de phishing, (aquellas que se dan a raíz de la interceptación de los datos vía la web y que no se necesita del plástico) las evidencias serán meramente digitales toda vez que desde que se inician los actos preparatorios hasta que se ejecutan se hacen a través del ciberespacio; aquí si hay que analizar direcciones IP, dominios, etc., para poder dar al traste con el ciberdelincuente y si habría que analizar a profundidad el o los dispositivos desde donde se producen los hechos.

3.2 Dificultades en la persecución

Con el pasar de los tiempos, el carácter transnacional del ciberdelito de clonación de tarjetas va adquiriendo mayor connotación. Esto se debe a que el delincuente puede estar físicamente en un lugar diferente al que se encuentre la víctima, ya sea persona física o entidad bancaria; incluso el delincuente puede recurrir al uso de redes de un tercer país y acarrear la afectación de bienes jurídicos de las diferentes jurisdicciones envueltas. Así, por ejemplo, se dan casos en donde un delincuente de un país roba datos bancarios a una persona ubicada en otro y que luego realiza compras en tiendas ubicadas en la web. Esto ha traído como resultado dificultades acerca de qué país tiene la competencia para perseguir, investigar y resolver el conflicto. Incluso, puede que también se trate de un grupo organizado que opere desde diferentes puntos, de aquí que la dificultad en la persecución además de la determinación del lugar se deba a la determinación del autor.

A tal efecto, la jurista española Mirentxu Corcoy Bidasolo, en torno a su publicación sobre "Problemática de la persecución penal de los denominados delitos informáticos": ha señalado que:

> la informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, resultando difícil determinar la autoría y el lugar de comisión del delito y, en consecuencia, la competencia para juzgar unos determinados hechos... Así, el problema esencial consiste en determinar la responsabilidad jurídico-penal de los intervinientes, y esclarecer cuál es la responsabilidad de los intermediarios de servicios[56].

En esa posición, debido a la incidencia e impacto de la comisión del ciberdelito de clonación de tarjetas en diversos lugares, y debido a que, por asuntos de soberanía nacional, los países no están facultados para intervenir con fines investigativos en otros estados sin la previa autorización, se hace imprescindible que los investigadores de los países involucrados ante la comisión de un ciberdelito busquen colaboración entre sí. En ese contexto**,** debido al carácter transnacional, la cooperación internacional, así como la asistencia legal mutua entre países, se consideran ser las principales herramientas que facilitan la persecución del delito tanto en su forma tradicional como aquellos que son considerados como delitos cibernéticos.

En esa misma línea, la oficialidad y requisitos que deben contener las solicitudes de colaboración internacional implica que el tiempo se convierta en un obstáculo para la investigación. Por lo general, se requiere que las respuestas se den en un tiempo corto cuando en la realidad, ante el gran auge y demanda de comisión de ciberdelitos, toma responder a la solicitud. Por lo que, es posible que datos que resulten ser necesarios para detectar el delito se borren rápidamente y no dé tiempo a su recolección.

Para Sabrina B. Lamperti, existen otros obstáculos a los cuales se enfrentan los que desarrollan investigaciones en materia de ciberdelitos, como: "…insuficiente capacidad para compartir los datos de la investigación, dificultades técnicas para rastrear los orígenes de los ciberdelincuentes, disparidad de capacidades de

[56] CORCOY BIDASOLO, Mirentxu. PROBLEMÁTICA DE LA PERSECUCIÓN PENAL DE LOS DENOMINADOS DELITOS INFORMÁTICOS: PARTICULAR REFERENCIA A LA PARTICIPACIÓN CRIMINAL Y AL ÁMBITO ESPACIO TEMPORAL DE COMISIÓN DE LOS HECHOS. *EGUZKILORE* [en línea]. 2007, (21), 7–32 [consultado el 10 de junio de 2022]. P.7. Disponible en: https://www.ehu.eus/documents/1736829/2176629/01+Corcoy.indd.pdf

investigación y capacidades forenses, escasez de personal bien preparado y una cooperación errática con otras partes responsables de la seguridad electrónica"[57].

A continuación, se analizarán los temas que consideramos más relevantes al momento de perseguir e identificar la jurisdicción competente y las alternativas que se tienen como soluciones ante tales problemáticas.

3.2.1 El caracter transnacional del ciberdelito de clonación de tarjetas e identificación de la jurisdicción competente

Como ya se ha establecido, mucho de los ciberdelitos se cometen fuera del territorio dominicano, de ahí que, una característica indiscutible de estos tipos de delitos es el hecho de que no existen barreras ni fronteras ni límites para que un delito cibernético sea cometido. Por tal razón, es común que la actuación delictiva que realiza un sujeto desde una nación produzca consecuencias en otras. Esto puede deberse a que el delincuente haya podido identificar brechas en un determinado país que le favorezcan ya sea, imposibilitando ser rastreado, perseguido y posteriormente ser procesado.

Es por ello que, el ciberdelito es considerado como un delito transnacional, es decir, no solo traspasa fronteras de países, sino que implican la afectación de bienes jurídicos comunes entre las diferentes naciones involucradas. En esta categoría pueden mencionarse delitos, tales como la trata o tráfico ilegal de personas, de armas y de drogas, entre otros.

Como resultado de la transnacionalidad, se ha sostenido la opinión de que una dificultad que suscita al momento de perseguir los ciberdelitos es precisamente el poder determinar o identificar cuál es la jurisdicción competente, ya que coexiste la posibilidad de que sea el lugar o país donde se inicia el acto, el lugar donde se

[57] LAMPERTI, Sabrina B. *Problemáticas en torno a la investigación de los delitos informáticos* [en línea]. 2014. Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática. Mar del Plata: Problemáticas en torno a la investigación de los delitos informáticos [consultado el 10 de junio de 2022]. P. 1. Disponible en: https://www.researchgate.net/publication/318983998_Problematicas_en_torno_a_la_investigacion_de_los_delitos_informaticos

concretiza o produce sus efectos el acto o donde estén establecidas las prestadoras de servicios de internet.

Resulta prudente exponer qué implican cada uno de estos renglones, comenzando por el lugar donde se inicia el acto. Para los partidarios de este renglón, la demarcación donde se inicia la ejecución, o, lo que es lo mismo, el lugar donde está ubicado el ciberdelincuente, es el competente para perseguir, investigar y condenar el hecho. Se extiende este criterio al manifestar, que el tribunal competente no solo sería donde el ciberdelincuente esté o comience a ejecutar su acto sino también "el servidor donde deja sus datos a disposición para que otras personas puedan revisarlos"[58]. Además, también según cita Claudia Cardenas a Cornils "se ha postulado incluso que quien sube datos a Internet no solamente actúa en el lugar donde se encuentra físicamente presente, sino que en todo Estado en el que los datos puedan ser accedidos a través de Internet"[59].

En segundo lugar, se encuentren aquellos que parten de la posición de que el tribunal competente debe ser aquel donde se ha consumado la infracción, o lo que es lo mismo, donde se produce el resultado, es decir, donde se encuentra la víctima y se lesiona el bien jurídico. Los que persiguen esta teoría, fundamentan su posición en que el derecho penal existe para proteger bienes jurídicamente protegidos**,** "en el desvalor de resultado"[60].

Hay una tercera postura que entiende que también puede ser competente el país donde se hayan producido diligencias que pudieran considerarse como de colaboración, como por ejemplo, los lugares o países en donde estén establecidas las prestadoras de servicios de internet. Sin embargo, la mayoría entiende que no puede ser competente un país en donde no se haya tenido ni un principio de ejecución ni de resultado, a menos que durante el simple curso causal de la acción esta represente un peligro.

[58]CÁRDENAS ARAVENA, Claudia. El lugar de comisión de los denominados ciberdelitos. *Política Criminal* [en línea]. 2008, (6), 1–14 [consultado el 1 de junio de 2022]. P. 7. Disponible en: https://repositorio.uchile.cl/bitstream/handle/2250/126580/Ellugardecomisiondelosdenominadosciberdelitos.pdf;sequence=1.
[59] Ibidem.
[60] BUSTOS RAMÍREZ, "Obras Completas", cit. nota n° 8, p. 404.

Como una teoría ecléctica, surge la teoría de la ubicuidad. Basados en esta teoría, el delito puede ser concebido como realizado tanto donde se produce el daño como donde se efectúa la conducta. Es decir, puede ser competente tanto en el país donde se ejecutó la acción como aquel en donde produjo sus resultados. Son muchos los doctrinarios que se inclinan por esta teoría y a juzgar por Esther E. Agelán Casasnovas "el denominado principio de ubicuidad ha sido creado por la jurisprudencia española como una solución práctica a los conflictos de jurisdicción en el conocimiento de los delitos cibernéticos"[61].

En cualquiera de los casos, es irrefutable que, ante la injerencia de diferentes países en relación a una misma conducta delictiva, surjan problemas jurisdiccionales con carácter internacional, por lo que, es necesario que se armonicen las leyes y los tratados sobre cooperación jurisdiccional sobre el ciberdelito y, que los Estados lo adopten como normativa, esto contribuiría positivamente en este contexto. En esa tesitura, a lo primero que interpelan los investigadores ante una investigación transnacional por ciberdelito, es que los países a los que se le requiera la asistencia y cooperación respondan de manera inmediata dada la naturaleza especial de los casos de delitos informáticos y la fragilidad de la prueba, requisito que muchas veces no se cumple.

3.2.2 Instrumentos de cooperación internacional en materia de persecución del ciberdelito de clonacion de tarjetas

El Convenio de Budapest aborda el tema de la cooperación internacional a partir de su artículo 23 y se basa en tres principios generales: principios generales relativos a la Cooperación Internacional, principios relativos a la Extradición, principios generales relativos a la Asistencia Mutua[62].

Resulta conveniente puntualizar aspectos importantes de estos principios y, comenzando por el principio general de cooperación internacional lo que el Convenio

[61] ANGELAN CASASNOVA, Esther E, (2011) ¨Ciberdelincuencia y Política Criminal¨, Internet: nuevo reto Jurídico. República Dominicana: Taller de Editora Premium, S.R.L. P. 74

[62] de Europa, C. (2001). Convenio sobre la Ciberdelincuencia. Consultado en: http://www. agpd. es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia. pdf.

explica es que las partes, es decir, los países, siempre que les sea posible deben colaborarse entre sí en todo lo que tenga que ver con las investigaciones o procedimientos en donde se encuentren envueltos sistemas de información incluyendo la obtención y recolección de evidencias digitales.

La cooperación internacional observa leyes nacionales armonizadas tanto sustantivas como procesales que penalizan e instituyen las normas que rigen los procedimientos, así como el manejo de la prueba, asimismo, observa instrumentos bilaterales, regionales y multilaterales sobre delitos informáticos. En consecuencia, es imprescindible que los países, se adhieran y ratifiquen cualquiera de estos instrumentos de manera que les sean vinculantes y con ello cuenten con armas necesarias para enfrentar o combatir la ciberdelincuencia y se puedan procesar los autores de tales delitos. Un requisito característico para que la cooperación internacional se otorgue es que se respeten las obligaciones internacionales en asuntos de derechos humanos.[63]

Otro principio que se convierte en instrumento para facilitar la investigación y procesamiento de delincuentes cibernéticos a través de la cooperación internacional es el de la extradición. En ese sentido, aquellas personas que cometan delitos de clonación de tarjetas desde un país, pero cuyos resultados se perciban en otro podrán ser objeto de extradición. Sin embargo, la extradición está sujeta a condiciones y puede ser negada de acuerdo a lo que esté previsto en el derecho interno del país solicitado o en los tratados de extradición que se encuentren vigentes.

La extradición es aplicable para los delitos establecidos desde el artículo 2 al 11 del Convenio de Budapest; el artículo 6 que regula el abuso de dispositivos y el artículo 8 que regula el fraude informático bajo los cuales se sanciona el delito de clonación de tarjetas, pero con la excepción de que el delito sea castigado en la legislación de los dos países implicados con penas de prisión como mínimo de un año. En la República Dominicana, la clonación es castigada con prisión de uno a diez años de prisión.

[63] Calvani, S., & Colombia, R. U. Rol de las Naciones Unidas (UNODC) en la lucha contra la delincuencia organizada transnacional, el terrorismo y la corrupción.

De acuerdo con la asistencia mutua, el artículo 25 de la Convención señala que los países firmantes se deben prestar "toda la ayuda mutua posible a efectos de las investigaciones o procedimientos" [64] o al manejo de pruebas surgidas a raíz de una infracción penal relacionadas a sistemas informáticos, telemáticos o de información, así como también. Asimismo, los estados están supuestos a acoger todas las medidas que entiendan oportunas para cumplir con las obligaciones respecto a los procedimientos de asistencia mutua donde no haya acuerdos internacionales aplicables, la asistencia mutua en materia de medidas provisionales, la asistencia mutua con relación al acceso de datos almacenados y la Red 24/7.

Como se ha establecido en párrafos anteriores, en muchos de los procesos sobre ciberdelitos en donde se requiere cooperación, las respuestas no son obtenidas con la rapidez que demandan este tipo de procesos debido a su naturaleza y las características propias del manejo de las pruebas digitales, por consiguiente, antes de que se adopten las medidas necesarias es muy probable que datos importantes hayan podido ser eliminados. Es por ello, que el mismo convenio, tratando de cubrir esta problemática indica que, en casos de urgencias, la solicitud de asistencia mutua pueda ser realizada a través de medios de comunicación que sean simples, breves, pero siempre que este constituya ser un medio seguro y auténtico, como, por ejemplo: el correo electrónico.

Las solicitudes de asistencia mutua deben ser presentadas de forma escrita incluyendo en su cuerpo información sobre quien requiere la asistencia, la razón de la solicitud, de la investigación o procedimientos a la que se refiere la solicitud, asimismo debe contener una descripción del delito o delitos, las leyes violadas, los procedimientos a seguir para la obtención conservación y, transferencia de las pruebas físicas y digitales a la autoridad que requiere la asistencia, los plazos para las solicitudes de conservación y ejecución de datos, así como otras informaciones que corroboren con el cumplimiento de la solicitud de asistencia al país que la solicita[65].

[64] de Europa, C. (2001). Convenio sobre la Ciberdelincuencia. Consultado en: http://www. agpd. es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_ Ciberdelincuencia. pdf.

[65] Colobran Huguet, M., Arqués Soldevila, J. M., & Guasch Petit, A. (2020). Análisis forense de sistemas de información, septiembre 2009.

A pesar de que hay países que contienen lineamientos y modelos respecto a las formalidades que deben cumplirse para las solicitudes de asistencia y las comisiones rogatorias (para aquellos donde no existen tratados ni acuerdos de cooperación internacional), esta no es una práctica que se da en todos los países. Es por ello que, la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) creó un programa que sirve de "Instrumento para redactar solicitudes de asistencia judicial (MLA- Mutual Legal Assistance) recíproca para ayudar a los profesionales de la justicia penal a redactar con prontitud las solicitudes de asistencia judicial recíproca, mejorando así la cooperación entre los Estados y acelerando las respuestas a esas solicitudes"[66]. En la República Dominicana, la ley designa como punto de contacto para la MLA (Mutual Legal Assistance) al DICAT.

Al igual que como pasa con la cooperación internacional y la extradición, la asistencia mutua también puede ser negada en algunos casos; por ejemplo, en procesos donde se perjudique el orden público y la soberanía cuando dicha asistencia implique violación de obligaciones internacionales en temas de derechos humanos del Estado que responde[67].

Por otra parte, el Artículo 35 del Convenio de Budapest establece la Red 24/7 como espacio de acercamiento disponible las 24 horas del día y los siete días de la semana como sistema de cooperación que facilite la obtención de pruebas electrónicas y digitales que indiquen la comisión de un delito, de una forma rápida avalando que el personal disponible dispone de la capacidad requerida y que cuenta con los recursos o equipos necesarios para el caso. La importancia de la Red 24/7 radica en que esta se utiliza como eje central ante las peticiones de conservación de la información y de asistencia mutua en investigaciones respecto a los ciberdelitos.

En la República Dominicana se ha establecido esta Red 24/7 como sistema conectado entre la Fiscalía y el DICAT para responder ante la asistencia jurídica inmediata que tengan que ver con investigaciones de crímenes y delitos de alta tecnología, así como también para solicitar evidencias digitales a otras autoridades

[66] James, J. I., & Gladyshev, P. (2016). A survey of mutual legal assistance involving digital evidence. Digital Investigation, 18, 23-32

[67] Calvani, S., & Colombia, R. U. Rol de las Naciones Unidas (UNODC) en la lucha contra la delincuencia organizada transnacional, el terrorismo y la corrupción.

mediante las redes de contacto de los países que han ratificado el Convenio de Budapest.

Llevando a práctica estos instrumentos de cooperación internacional, en el año 2020 fueron detenidos en el aeropuerto de Madrid, España, dos personas de nacionalidad rumana que lideraban una red dedicada a clonar tarjetas bancarias a través de la modalidad "skimming". Esta operación contó con la cooperación de Colombia, Venezuela, República Dominicana y Rumanía porque esta organización criminal de alguna manera afectó intereses de cada uno de estos estados[68].

3.3 Desarrollo de la ciberseguridad en la República Dominicana

Este flagelo cibernético ha desatado un nuevo desafío: desarrollar medidas de seguridad que procuren garantizar o proteger la confianza y privacidad digital de los usuarios de sistemas de información y comunicación. De manera que, tanto las instituciones públicas como las privadas y los usuarios individuales se han visto en la necesidad de invertir y seguir protocolos de ciberseguridad a fin de que los datos, servicios o productos que ofrezcan a través del internet no se vulneren ante la comisión de un ciberdelito.

Carlos Leonardo, desde el Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD) ha manifestado que "cualquier organización con activos digitales tiene el potencial de experimentar un ataque cibernético. Desafortunadamente, gran parte de las organizaciones no se dan cuenta de que han experimentado una filtración de datos hasta que es demasiado tarde. La creación de un plan de respuesta a incidentes de ciberseguridad ayuda a prepararse para lo inevitable y a equipar a el equipo de seguridad para responder antes, durante y después de un ataque cibernético"[69].

[68] EUROPA PRESS. Detenidos los jefes de una banda que clonaba tarjetas instalando dispositivos en cajeros automáticos. *europapress.es* [en línea]. 24 de febrero de 2020 [consultado el 10 de marzo de 2022]. Disponible en: https://www.europapress.es/madrid/noticia-detenidos-jefes-banda-clonaba-tarjetas-instalando-dispositivos-cajeros-automaticos-20200224110309.html

[69] La Ciberseguridad en la Republica Dominicana 2021. *Centro Nacional de Ciberseguridad* [en línea]. 18 de enero de 2021 [consultado el 15 de mayo de 2022]. P. 21. Disponible en: https://cncs.gob.do/wp-content/uploads/2022/01/La-Ciberseguridad-en-la-República-Dominicana-2021.pdf

Hasta el momento el problema mayor radica en el tiempo en que tardan en desarrollarse estos lineamientos de seguridad. Y es que nos enfocamos más en el uso o incluso la creación de nuevas tecnologías que se nos olvida anticipar medidas de seguridad desde el inicio de la creación de la nueva tecnología que ayuden a reducir las brechas que faciliten la comisión de un eventual ciberataque.

Sin embargo, para establecer con precisión la posición que ocupa la República Dominicana respecto a los niveles de ciberseguridad, se debe partir del año 2016 con el proyecto gubernamental República Dominicana Digital, a través del cual se buscó reducir la brecha digital existente en la ciudadanía dominicana y brindar accesos a las tecnologías de la información y comunicación. A partir de este punto, el país en conjunto con la Organización de Estados Americanos (OEA) comenzó a trabajar el tema de la ciberseguridad y la protección de infraestructuras críticas, redactando una Estrategia Nacional de Ciberseguridad, que posteriormente el 19 de junio del 2018 fue aprobada mediante decreto presidencial marcado con el No. 230-18.

A través del decreto No. 238-18 sobre Estrategia Nacional de Seguridad Cibernética, se instituyeron los mecanismos de ciberseguridad que debían ser acogidos, para que el Estado estuviera en condiciones de poder prevenir, detectar y gestionar eventualidades surgidas a través del uso de los sistemas de información del Estado y en las infraestructuras críticas nacionales, de manera que, el país contara con líneas de acción claras respecto a la política pública de ciberseguridad en la República Dominicana, para protección del propio Estado y de sus integrantes en general.

Asimismo, este decreto crea el Centro Nacional de Ciberseguridad y como una dependencia que opera dentro de este, un Equipo Nacional de Respuesta e Incidentes de Seguridad Informática, (C-SIRT son sus siglas en inglés). Desde su creación, el Centro Nacional de Ciberseguridad precisó su estrategia basada en un análisis de datos estadísticos como una manera de obtener resultados de gran impacto en menos tiempo y de vislumbrar las particularidades más significativas respecto a la realidad de la ciberseguridad en el estado dominicano.

Con el Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD), se incorporan los primeros lineamientos de protección frente a todo tipo de amenaza que se

de en el ciberespacio, colocando a merced del público servicios en línea, informes de vulnerabilidad, notificaciones de alerta, boletines y guías informativas contribuyendo, por tanto, con la formación de una cultura en ciberseguridad. Respecto a este punto, hay que hacer mención de que también se establecieron otras unidades sectoriales especializadas, como son el CSIRT del sector financiero y el CSIRT del Ministerio de Defensa, los cuales hoy por hoy se encuentran en función y se encargan de dar asistencia en sus respectivas áreas.

Es indudable que la República Dominicana ha ido cosechando buenos frutos sobre lo que ha ido sembrando en materia de ciberseguridad. Esto se recoge en los últimos resultados dados a conocer en el año 2021, a través de la cuarta edición del informe sobre el "Índice Global de Ciberseguridad (GCI) 2020", el cual evalúa el compromiso y desarrollo de los países que forman parte de la Unión Internacional de Telecomunicaciones (UIT) respecto a la concientización de las amenazas cibernéticas y a la ciberseguridad a nivel global en base a: las medidas legales, técnicas, y organizativas, de cada país así como también el desarrollo de capacidades, y la cooperación con otros países.

De acuerdo al último Índice Global de Ciberseguridad presentado por la Unión Internacional de Telecomunicaciones (UIT)[70] la República Dominicana subió 26 lugares desde la posición que ocupaba en el 2018 y, de la posición No. 92 pasó a ocupar la No. 66 de los 182 países que participaron en el cuestionario, obteniendo una puntuación de 75.05 a nivel global. A nivel de la región de Las Américas, avanzó desde la posición No. 10 a la No. 6 entre los 35 países que la conforman y, obtuvo una calificación de 75.07.

Con esta publicación queda demostrado, que gracias al esfuerzo y coordinación hecho por el Centro Nacional de Ciberseguridad y los diferentes sectores del país, tanto del ámbito público como privado, que tienen incidencia en la elaboración, marcha y cumplimiento de políticas y estrategias de ciberseguridad, el país ha logrado posicionarse con un notable avance en el compromiso con la ciberseguridad estableciendo iniciativas y programas concretos en ciberseguridad, así como una mejora

[70] BOGDAN-MARTIN, Doreen. ITU Publications. *ITU: Committed to connecting the world* [en línea]. 2022 [consultado el 10 de mayo de 2022]. Disponible en: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

continua en el fortalecimiento de los ejes que conforman la Estrategia Nacional de Ciberseguridad.

En otro orden, durante el 2021, en conjunto con la Organización de los Estados Americanos (OEA) y la Unión Europea, el país desarrolló un programa de formación y sensibilización especializada alineada al desarrollo de una cultura de ciberseguridad que incluye tanto a los equipos sectoriales de respuestas a incidentes cibernéticos como también a las unidades de seguridad cibernéticas de las entidades del gobierno, y que enfoca al país hacia una posición adelantada respecto al mejoramiento de sus prácticas. Otro elemento que ha sido clave para el fortalecimiento y avance del país han sido la adopción de mecanismos de cooperación y alianzas tanto a nivel interno como internacional.

A nivel gubernamental, así como el gobierno de turno propuso el cambio a una República Digital a través del uso de las TIC´s, debe también responder ante las vulnerabilidades del sistema. En ese sentido, el gobierno debe contar con los mecanismos necesarios que protejan el ciberespacio, fortalezcan las instituciones en materia de ciberespacios seguros y de ciberseguridad para todos los usuarios de la red; de aquí que la ciberseguridad sea el eje transversal de la Agenda Digital 2030.

La Agenda Digital 2030, es un proyecto del Gabinete de Transformación Digital, mediante el cual el gobierno dominicano ha asumido como su prioridad al más alto nivel la obligación de promover y mejorar todo lo concerniente a la ciberseguridad, con el fin de proteger no solo a las instituciones o sectores productivos del país sino a toda la colectividad a través de la promoción de labores en favor de un ciberespacio más confiable y seguro.

En lo que tiene que ver con el contexto jurídico y normativo en materia de ciberdelitos y ciberseguridad, el 2021 simbolizó significativas mejoras para la República Dominicana, puesto que salieron a la luz varios proyectos de ley que encaminan el fortalecimiento de los instrumentos legales con los que cuenta el país para prevenir, perseguir y combatir de manera efectiva todo lo que tiene que ver con delitos cibernéticos.

A pesar de que la República Dominicana fue uno de los primeros países de la región en adherirse al Convenio de Budapest y también en contar con una legislación contra la ciberdelincuencia, esta resulta ser anticuada para los nuevos tiempos pues, han pasado ya 15 años desde su promulgación. Al menos en la actualidad se habla de su modificación, ya que como las infracciones a través de tecnologías son tan cambiantes, urge tipificar y sancionar nuevas conductas delictivas que han ido surgiendo en el devenir de estos años.

En el año 2021 también fue sometido al Congreso Nacional un anteproyecto de Ley sobre Gestión de la Ciberseguridad en República Dominicana a través del cual se busca regular, prevenir, gestionar y responder a las amenazas e incidentes de ciberseguridad y también otros temas concernientes a la seguridad cibernética en el país.

En materia de alianzas y cooperación a nivel internacional, el país logró establecer acuerdos con compañías líderes a nivel mundial en dar amplias soluciones a temas de ciberseguridad, como, por ejemplo: Fortinet. Mediante este acuerdo la empresa Fortinet apoyará al país en las áreas de capacitación, intercambio de conocimientos tecnológicos y de información estratégica sobre amenazas relacionadas con la ciberseguridad. Asimismo, suscribió un acuerdo de cooperación con la empresa Microsoft para mejorar las competencias del país con el tema de la ciberseguridad.

A nivel nacional, el Centro Nacional de Ciberseguridad y CLARO Dominicana, suscribieron un acuerdo mediante el cual la prestadora de servicio se comprometió a apoyar al Estado en temas tecnológicos e intercambio de estrategias sobre materia de ciberseguridad. El principal objetivo del acuerdo es "gestionar de manera adecuada el panorama de riesgo tecnológico del ciberespacio dominicano ante el proceso de transformación digital que existe, fortaleciendo las capacidades de respuesta y recuperación ante ataques cibernéticos a instituciones críticas nacionales, propiciando el intercambio de inteligencia cibernética, la gestión de vulnerabilidades técnicas y realizando labores de concientización y capacitación"[71].

[71] El Ministerio de la Presidencia firma alianza con Claro para colaboración técnica en ciberseguridad – Ministerio de la Presidencia. *Ministerio de la Presidencia – Sitio Web Institucional del Ministerio de la Presidencia de la República Dominicana* [en línea]. 28 de octubre de 2021 [consultado el 10 de abril de 2022]. Disponible en: https://minpre.gob.do/comunicacion/notas-de-prensa/el-ministerio-de-la-presidencia-firma-alianza-con-claro-para-colaboracion-tecnica-en-ciberseguridad/

Para fines de esta investigación, sobre la clonación de tarjetas bancarias en la República Dominicana, el campo de desarrollo en el tema ciberseguridad que más interesa es el que ha tenido lugar en el sistema financiero y de pagos del país. Respecto a este, en el año 2018, La Junta Monetaria aprobó el Reglamento de Seguridad Cibernética y de la Información y, para el año 2019 emitió su instructivo de aplicación común para los bancos de ahorro, crédito, múltiples, asociaciones de ahorros y préstamos y entidades de intermediación financiera y de pagos, y cualquier otro tipo de entidad que la Junta Monetaria autorice en el futuro. Estos reglamentos fueron implementados durante el año 2020 y, gracias al conjunto de estas acciones, el 2021 fue de importantes resultados ya que se crearon planes para su fortalecimiento de acuerdo a los niveles de riesgos, y así aminorar en corto tiempo los peligros relacionados a la ciberseguridad tanto para cada entidad bancaria o financiera como para el sistema económico como un todo.

Finalmente, se debe establecer que para cualquier área que implique desarrollo de un país, entiéndase: educación, turismo, comercio, entre otras, es necesario e imprescindible el uso de las tecnologías de la información y comunicación, que, así como dan paso a un universo infinito de conocimientos y oportunidades también lo hacen con temas que implican riesgos y amenazas. Estas amenazas y riesgos son cada vez tan sofisticados, avanzados y comunes que constituyen una alta inseguridad para cualquier persona o país pudiendo verse afectada, incluso, la seguridad nacional. La única manera de hacer frente es a través del manejo de buenas prácticas en el ámbito de la ciberseguridad, las cuales se logran a través de esfuerzos aunados a nivel nacional, regional y mundial en la búsqueda de prevenir y responder a los ataques cibernéticos de forma efectiva, y sobre los cuales hay que mantenerse siempre actualizados y fortalecidos debido a las constantes variaciones que existen a nivel cibernético.

Conclusión y recomendaciones

En esta investigación se indagó acerca del ciberdelito de clonación de tarjetas en la República Dominicana, los métodos utilizados por los ciberdelincuentes, el impacto de este a partir el año 2020 producto del COVID-19 así como también, el desarrollo de la ciberseguridad en nuestro país para determinar qué medidas se pueden tomar a fin de evitar o combatir la comisión de este tipo de crímenes-delitos.

La importancia de esta investigación radicó no solo en las graves afectaciones que se generan al patrimonio económico de las personas y las instituciones bancarias y financieras, a través de las clonaciones de tarjetas, sino también por la incidencia que tiene en la economía nacional y, en mucho de los casos, por su vinculación con esquemas relativos a crímenes organizados transnacional. Dicho esto, la investigación y persecución de estos delitos debe alcanzar, además de la afectación al patrimonio de las personas tanto físicas (tarjeta habiente) como morales (instituciones financieras), la seguridad económica del Estado dominicano.

A continuación, se presentan las conclusiones, avances y las recomendaciones más importantes sugeridas a raíz de esta investigación.

Lo primero que se debe decir es que, ha quedado claro que cada vez más el uso de dispositivos electrónicos y tecnologías de la información y de la comunicación constituyen una práctica en auge tanto por las empresas y/o instituciones como a nivel personal. Durante el año 2020, la anhelada evolución digital se apresuró debido a la crisis del COVID-19. Esto, obligó a todos a estar en sus hogares y valerse de la virtualidad para todos sus quehaceres cotidianos, situación que los cibercriminales aprovecharon y aumentaron como nunca antes sus ciberataques, lo que resultó en un crecimiento exitoso de esta industria ilegal.

Es decir, todo ocurrió de forma tan inesperada que los cibernautas olvidaron tener en cuenta las medidas de seguridad necesarias. Y si bien, siempre existirá la brecha no menos cierto es que existe una variedad de programas incluso libres de costo y fáciles de usar que posibilitan que cualquier persona logre proteger sus datos electrónicos, ya sea a través de la encriptación de sus mensajes, de programas antivirus o cualquier otro. No

obstante, lo que sucede es que, pese a los avances, no es asumida la suficiente educación sobre ciberseguridad o seguridad en internet que todo aquel usuario de la red debe asumir mientras que por el contrario, los ciberdelincuentes van sofisticando cada día más sus técnicas.

Es por ello que, así como es trascendental conocer sobre ciberdelincuencia también lo es saber sobre ciberseguridad, de manera tal que no quede duda alguna de cómo operan estos tipos de delincuentes, pero más aún de cómo protegernos de ellos y así saber cómo se debe proceder. De igual forma, y como el ciberdelito es un delito que no tiene fronteras ni límites, se deben encaminar acciones a nivel global de manera que las consecuencias que se deriven apliquen para las diferentes naciones y los ciberdelitos puedan ser correctamente perseguidos y sancionados.

En ese sentido, se requiere de la colaboración y asistencia de los diferentes Estados, gobiernos, de cualquier entidad bien sea pública o privada, en fin, de la sociedad en general, toda vez que, por la complejidad de la delincuencia cibernética se necesitan de esfuerzos mancomunados si se quiere que la misma no suponga un peligro jurídico ni social.

Además, como crimen organizado, deben tomarse acciones relativas al estudio de los grupos que lo conforman ya que esto supone un obstáculo para la persecución. Dependiendo de la modalidad, existen diferentes grupos delictivos y por lo general las autoridades no se detienen a analizarlos, lo que hace que no puedan identificarse perfiles para determinar posibles orígenes de la criminalidad.

Sin duda alguna, la República Dominicana ha sido proactiva en estos temas pues ha encaminado acciones tales como conferencias para identificar nuevas modalidades de delitos, necesidades emergentes, también para intercambiar información y conocimientos. De igual forma, se han realizado diversas capacitaciones tratando de crear conciencia en la sociedad con el objetivo de prevenir la ciberdelincuencia. Asimismo, se han firmado convenios de cooperación en ciberseguridad, lo que ha hecho que el país haya reforzado ampliamente su postura en conocimientos y manejo de técnicas de seguridad cibernética y ocupe mejor posición que en años anteriores.

Sin embargo, a pesar de los innegables avances siguen existiendo necesidades para afrontar la brecha cibernética, en ese sentido, entendemos que las siguientes recomendaciones son elementos claves que deben, desde el ámbito legislativo, sustantivo como procesal, así como desde la cooperación internacional, implementarse lo antes posible, ya que el creciente auge digital exige medidas y consecuencias acordes a la modalidad de delito, pero al mismo tiempo accesibles y fáciles de utilizar.

En ese sentido, y para comenzar, se pudo evidenciar que la actual ley que tipifica y sanciona los delitos cibernéticos, Ley 53-07, necesita con urgencia ser modificada. Hoy por hoy existen nuevas modalidades de cometer ciberdelitos y si no hay una ley que las tipifique no puede haber ninguna persecución contra estos. Debe mencionarse que el actual presidente de la República, Luis Abinader, en fecha 14 de junio de 2022, remitió al Congreso Nacional un proyecto de ley contra la ciberdelincuencia, para adecuarse a las nuevas conductas y tendencias del ciberdelito, así como para agravar el tiempo de las condenas y regular el tema de la preservación de evidencia digital, el decomiso de bienes, la competencia jurisdiccional y la acción pública. Sin embargo, este proyecto fue retirado del Congreso en menos de un mes. Aún así, esperamos que en la brevedad posible sea nueva vez introducido ya que persiste la necesidad de reforma a la ley.

En esa misma línea, actualmente el delito de clonación de tarjetas es de acción pública a instancia privada, es decir, que el ministerio público ejerce su acción una vez haya sido interpuesta una denuncia o querella. Sin embargo, entiendo que este delito debe ser público porque a través de estos no se afecta solo el patrimonio económico de las personas afectadas o de la entidad bancaria sino también que se afecta el orden socioeconómico del país porque las entidades bancarias, como parte del sistema financiero, sustentan su crecimiento, desarrollo y estabilidad económica y financiera. En ese mismo orden, deben incluirse agravantes[72] que puedan ser tomadas en cuenta, por ejemplo, dependiendo del monto afectado o de la relación entre el clonador, la víctima, la institución, por ejemplo, si el autor es empleado bancario, entre otros.

En otro orden, los sujetos que forman parte de las entidades encargadas de la investigación y persecución de los ciberdelitos deben ser suficientes. En la actualidad, en

[72] ANGELAN CASASNOVA, Esther E, (2011) ¨Ciberdelincuencia y Política Criminal¨, Internet: nuevo reto Jurídico. República Dominicana: Taller de Editora Premium, S.R.L.

la provincia de Santiago no existe el personal suficiente para dar respuestas a los casos. Como sabemos, el personal que conforma estos departamentos tiene que disponer de ciertos conocimientos y expertiz, por tanto, debe tenerse un banco de elegibles que el mismo Estado se haya encargado de estar capacitando para que no haya falta de recurso humano, que es el recurso más importante en estas dependencias.

Urge también, que en más provincias haya departamentos especializados para investigar este tipo de casos porque no en todas encontramos un DICAT ni una fiscalía exclusiva para tratar temas ciberdelitos.

Respecto al proceso, este es muy burocrático. Comenzando con que si se lleva por la jurisdicción penal, para cada actuación el ministerio público debe solicitar autorización al juez, también porque a veces las víctimas llevan procesos penales paralelos a otros llevados por ante la Superintendencia de Bancos lo que resulta tedioso para la víctima y esta termina desanimándose o desistiendo, esto hace que muchos procesos no lleguen hasta el final y no se condenen porque si la parte víctima obtuvo respuesta de la Superintendencia de Bancos raras veces continúa ante la jurisdicción penal o viceversa. Se deben encaminar esfuerzos para que estos procesos a pesar, de ser delicados, se puedan llevar en un plazo prudente, tanto por todas las solicitudes y formalidades que hay que cumplir como también por lo del manejo de evidencias, pero sobre todo por el bien jurídico protegido que se afecta a través de la clonación de tarjetas: el patrimonio económico.

Se recomienda que el Estado, en su agenda, le de la importancia que requiere el Centro Nacional de Ciberseguridad y se empleen los presupuestos necesarios para que ellos puedan disponer de la tecnología de poder cuidar todas las infraestructuras críticas del país. Igualmente, se exhorta a seguir invirtiendo e implementando estrategias y mecanismos que desarrollen los grados de conocimiento en seguridad cibernética entre los ciudadanos, las empresas, las instituciones gubernamentales, pero también a nivel internacional para que sean menos vulnerables a ciberdelitos, para mejorar la eficacia de los procesos y como una respuesta global a la problemática

A nivel personal, se les recomienda a los ciudadanos estar siempre al pendiente de su plástico y/o de los sitios webs a los que acceda, asimismo que le dé un seguimiento

más cercano a los movimientos reflejados en su estado de cuenta, de manera que puedan identificar lo antes posible si han sido víctima de clonación o de uso indebido de sus fondos. Se recomienda también, que además de modificar frecuente sus contraseñas o códigos de accesos, utilicen códigos más seguros; a no dar información personal por ninguna vía, ni por teléfono, ni por correo, a no ser que sepa con seguridad quién es la persona con la que está compartiendo la información. Tampoco dejar datos bancarios guardados ni en teléfonos ni en computadoras.

Respecto a las entidades bancarias, se les recomienda invertir en mejoras para reforzar los mecanismo de seguridad de sus infraestructuras y de las plataformas virtuales mediante las cuales ofrecen sus productos y servicios, para que sean más seguras y no se puedan violar tan fácil, de tal forma que se evite que las víctimas entreguen sus datos personales y que sean víctimas de fraudes cibernéticos. En ese aspecto, se podría implementar como mecanismo de seguridad la doble verificación, es decir, que el usuario cuente con dos pasos para acceso a sus productos. También, que implementen protocolos para activar alarmas en caso de que sean atacadas las infraestructuras. Así mismo, se le recomienda, seguir formando al personal que labora en sus dependencias, ya que además de verse económicamente afectados también pierden la credibilidad de su imagen y esto se convierte en un perjuicio económico.

Finalmente, se debe decir que el ciberdelito de clonación de tarjetas, es un hecho que al igual que cualquier otro tipo de delito, no será suprimido del todo. Sin embargo, lo indispensable es crear la conciencia acerca de las herramientas disponibles tanto a nivel personal como legal, para así minimizar cualquier tipo de ciberataque.

Glosario De Términos

A

Artilugios: Mecanismo, artefacto, sobre todo si es de cierta complicación

Adware: Son programas que recopilan información acerca de los hábitos de navegación del usuario en cuestión para luego mostrar publicidad

B

Blanqueo: Consiste en ocultar o encubrir el origen de beneficios obtenidos ilícitamente, de forma que parezcan provenir de fuentes legítimas.

Bots: Es un programa informático que efectúa automáticamente tareas reiterativas mediante Internet a través de una cadena de comandos o funciones autónomas previas para asignar un rol establecido; y que posee capacidad de interacción, cambiando de estado para responder a un estímulo

C

Cyberbulling: Es acoso o intimidación por medio de las tecnologías digitales.

Ciberdelito: Delito que se comete a través de internet.

Ciberdelincuencia: Actividad delictiva que se lleva a cabo a través de internet.

Ciberstalking: Consiste en el uso de Internet u otros medios electrónicos para acechar o acosar a un individuo, grupo u organización. Puede incluir acusaciones falsas, difamación, calumnias y calumnias. También puede incluir monitoreo, robo de identidad, amenazas, vandalismo, solicitud de sexo, o chantaje.

Consola: Dispositivo que, integrado o no en una máquina, contiene los instrumentos para su control y operación

D

Digitalizado: Convertir o codificar en números dígitos datos o informaciones de carácter continuo, como una imagen fotográfica, un documento o un libro.

DoS: Son las siglas de Disk Operating System, "Sistema Operativo de Disco" o "Sistema Operativo en Disco", es una familia de sistemas operativos para computadoras personales (PC).

E

Encriptar: Es una forma de ocultar información dentro de otra información, de tapar un mensaje a simple vista. Es una forma de codificar información de manera que si alguien la intercepta no sea capaz de leerla con acierto.

G

Grooming: Es la acción deliberada de un adulto, varón o mujer, de acosar sexualmente a una niña, niño o adolescente a través de un medio digital que permita la interacción entre dos o más personas, como por ejemplo redes sociales, correo electrónico, mensajes de texto, sitios de chat o juegos en línea.

H

Hackear: Introducirse de forma no autorizada en un sistema informático.

I

Internet: Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

Ingeniería: Arte y técnica de aplicar los conocimientos científicos a la invención, diseño, perfeccionamiento y manejo de nuevos procedimientos en la industria y otros campos de aplicación científicos.

K

Kits: Conjunto de elementos necesarios para realizar el montaje completo de un aparato, software, producto o servicio.

M

Malware Es un término genérico utilizado para describir una variedad de software hostil o intrusivo: virus informáticos, gusanos, caballos de Troya, software de rescate, spyware, adware, software de miedo, etc. Puede tomar la forma de código ejecutable, scripts, contenido activo y otro software.

N

Navegadores: Son programas que permiten ver la información que contiene una página web. El navegador interpreta el código, HTML generalmente, en el que está escrita la página web y lo presenta en pantalla permitiendo al usuario interactuar con su contenido y navegar.

P

Pharming: Es un tipo de ciberataque donde el atacante que implementa esta técnica, intenta redirigir el tráfico web, especialmente los datos de solicitud, a un sitio web fraudulento.

Phishing: Es una técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo.

S

Sextorsión: Consiste en la amenaza de revelar información íntima sobre una víctima a no ser que esta pague al extorsionista.

Sistema: Es el conjunto de partes interrelacionadas: hardware, software y personal informático, que permite almacenar y procesar información.

T

Tecnología:
Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del cono cimiento científico.

V

Virus: Es un software que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario principalmente para lograr fines maliciosos sobre el dispositivo.

Virtualidad: Que está ubicado o tiene lugar en línea, generalmente a través de internet.

Referencias bibliográficas

1. ACURIO DEL PINO, Santiago. Delitos informáticos: generalidades. 2016. [en línea]. Ecuador. [Consultado el 2 de marzo de 2021]. Disponible en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
2. ANGELAN CASASNOVA, Esther E, (2011) ¨Ciberdelincuencia y Política Criminal¨, Internet: nuevo reto Jurídico. República Dominicana: Taller de Editora Premium, S.R.L.
3. ATHAL, Krishna. La correlación entre Covid-19 y el ciberdelito. Entrepreneur [en línea]. 22 de marzo de 10 [consultado el 8 de mayo de 2022]. Disponible en: https://www.entrepreneur.com/article/421994
4. Aumenta el cibercrimen en República Dominicana en el contexto de COVID-19. Hoy Digital [en línea]. 06 de mayo de 2020 [consultado el 8 de mayo de 2022]. Disponible en: https://hoy.com.do/aumenta-el-cibercrimen-en-republica-dominicana-en-el-contexto-de-covid-19/
5. BAUTISTA, Félix. La expresión y la intimidad. listindiario.com [en línea]. 2 de mayo de 2012 [consultado el 28 de mayo de 2022]. Disponible en: https://listindiario.com/puntos-de-vista/2012/05/02/230920/la-expresion-y-la-intimidad
6. BATUECAS CALETRIO, A. (2005). Pago con tarjeta de crédito. Naturaleza y régimen jurídico. Cizur Menor: Aranzadi.
7. BOGDAN-MARTIN, Doreen. ITU Publications. *ITU: Committed to connecting the world* [en línea]. 2022 [consultado el 10 de mayo de 2022]. Disponible en: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E
8. BUSTOS RAMÍREZ, "Obras Completas", cit. nota n° 8.
9. CAMACHO CASTILLO, Miguel Angel. Solución de estrategia empresarial dominios de nivel superior para mitigar el fraude electrónico (PHISHING) en la banca electrónica por internet, Mexico, 2016.
10. CÁRDENAS ARAVENA, Claudia. El lugar de comisión de los denominados ciberdelitos. *Política Criminal* [en línea]. 2008, (6), 1–14 [consultado el 1 de junio de 2022]. Disponible en: https://repositorio.uchile.cl/bitstream/handle/2250/126580/Ellugardecomisiondelosdenominadosciberdelitos.pdf;sequence=1.

11. Calvani, S., & Colombia, R. U. Rol de las Naciones Unidas (UNODC) en la lucha contra la delincuencia organizada transnacional, el terrorismo y la corrupción.

12. CORCOY BIDASOLO, Mirentxu. PROBLEMÁTICA DE LA PERSECUCIÓN PENAL DE LOS DENOMINADOS DELITOS INFORMÁTICOS: PARTICULAR REFERENCIA A LA PARTICIPACIÓN CRIMINAL Y AL ÁMBITO ESPACIO TEMPORAL DE COMISIÓN DE LOS HECHOS. *EGUZKILORE* [en línea]. 2007, (21), 7–32 [consultado el 10 de junio de 2022]. Disponible en: https://www.ehu.eus/documents/1736829/2176629/01+Corcoy.indd.pdf

13. COLOBRAN HUGUET, M., Arqués Soldevila, J. M., & Guasch Petit, A. (2020). Análisis forense de sistemas de información, septiembre 2009.

14. Consejo de Europa, Convenio Sobre la Ciberdelincuencia, Budapest. 2001.

15. CORTEZ, Carlos. Delito fácil y barato. El Mañana [en línea]. 26 de noviembre de 2012 [consultado el 8 de marzo de 2022]. Disponible en: https://www.elmanana.com/delito-facil-y-barato/1860062

16. Council of Europe (2020) en CASTILLO RUBIANO, Oscar. (2021). Phishing: Día de Pesca. Colombia.

17. del Pino, S. A. (2019). Manual de manejo de evidencias digitales y entornos informáticos. Versión 2.0.

18. DIAZ VALDEMAR, Miguel. El ciberdelito una actividad rentable en la República Dominicana. *El Nuevo Diario (República Dominicana)* [en línea]. 18 de marzo de 2022 [consultado el 10 de mayo de 2022]. Disponible en: https://elnuevodiario.com.do/el-ciberdelito-una-actividad-rentable-en-la-republica-dominicana/

19. de Europa, C. (2001). Convenio sobre la Ciberdelincuencia. Consultado en: http://www. agpd. es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia. pdf.

20. de Europa, C. (2001). Convenio sobre la Ciberdelincuencia. Consultado en: http://www. agpd. es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia. pdf.

21. ENCALADA OCHOA, Graciela. *A CRIMINALIDAD INFORMÁTICA: PROPUESTA PARA LA TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS EN LA LEGISLACIÓN ECUATORIANA*. Maestría, Cuenca, 2010 [consultado el 16 de abril de 2022]. Disponible en: tm4328.pdf

22. EUROPA PRESS. Detenidos los jefes de una banda que clonaba tarjetas instalando dispositivos en cajeros automáticos. *europapress.es* [en línea]. 24 de febrero de 2020 [consultado el 10 de marzo de 2022]. Disponible en: https://www.europapress.es/madrid/noticia-detenidos-jefes-banda-clonaba-tarjetas-instalando-dispositivos-cajeros-automaticos-20200224110309.html

23. El Ministerio de la Presidencia firma alianza con Claro para colaboración técnica en ciberseguridad – Ministerio de la Presidencia. *Ministerio de la Presidencia – Sitio Web Institucional del Ministerio de la Presidencia de la República Dominicana* [en línea]. 28 de octubre de 2021 [consultado el 10 de abril de 2022]. Disponible en: https://minpre.gob.do/comunicacion/notas-de-prensa/el-ministerio-de-la-presidencia-firma-alianza-con-claro-para-colaboracion-tecnica-en-ciberseguridad/

24. GERCKE,Dr. Marco. *Comprensión del Ciberdelito: Fenómenos, Dificultades y Respuesta Jurídica*. [en línea]. UIT, 2014. [Consultado en 17/03/2021]. P. 11. Disponible en: Libro UIT CybcrimeS | PDF | Tecnología de información y comunicaciones | La seguridad informática (scribd.com)

25. GRISALES PÉREZ, Giovanni. Análisis dogmático de las conductas de Hurto por medios informáticos y semejantes (Art. 269i) y Transferencia no consentida de activos (Art. 269j) Ley 1273 de 2009. 2013. Universidad EAFIT. Maestría en Derecho Penal. [consultado el 8 de marzo de 2021]. Disponible en: https://repository.eafit.edu.co/bitstream/handle/10784/1285/GrisalesPerez_GiovanniSaltin_2013.pdf;jsessionid=571C398EF368860555CC7EAB75C67E29?sequence=1

26. JAMES, J. I., & Gladyshev, P. (2016). A survey of mutual legal assistance involving digital evidence. Digital Investigation, 18, 23-32

27. JARAMILLO ACEVEDO, Mariela. & ZAMBRANO, María. Migración de banda magnética a chip para evitar fraudes de clonación de tarjetas de crédito o débito. ¿los bancos ecuatorianos están preparados para este cambio? Guayaquil, Ecuador, 2013.

28. JIJENA, Renato**.** Chile, la protección penal de la intimidad y el delito informático. Editorial Jurídica de Chile. 1ª Edición, 1992.

29. LAMPERTI, Sabrina B. *Problemáticas en torno a la investigación de los delitos informáticos* [en línea]. 2014. Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática. Mar del Plata: Problemáticas en torno a la investigación de los delitos informáticos [consultado el 10 de junio de 2022]. P. 1. Disponible en: https://www.researchgate.net/publication/318983998_Problematicas_en_torno_a_la_investigacion_de_los_delitos_informaticos

30. La Ciberseguridad en la Republica Dominicana 2021. *Centro Nacional de Ciberseguridad* [en línea]. 18 de enero de 2021 [consultado el 15 de mayo de 2022]. P. 21. Disponible en: https://cncs.gob.do/wp-content/uploads/2022/01/La-Ciberseguridad-en-la-República-Dominicana-2021.pdf

31. La investigación que realiza el criminólogo-criminalista en la clonación de tarjetas bancarias. P. 46. http://revista.cleu.edu.mx/new/descargas/1301/articulos/03_La_investigacion_que_realiza_el_criminologo-criminalista_en_la_clonacion_de_tarjetas_bancarias.pdf

32. Ley de Ciberseguridad se adheriría a Convenio de Budapest sobre ciberdelincuencia. Noticias Cholusat Sur [en línea]. [sin fecha] [consultado el 8 de julio de 2022]. Disponible en: http://cholusatsur.com/ley-de-ciberseguridad-se-adheriria-convenio-de-budapest-sobre-ciberdelincuencia/

33. MARIANA LEGUIZAMÓN, Mayra Sheyla. EL PHISHING. Tesis de grado, Universitat Jaume. [sin fecha] [consultado el 3 de marzo de 2021]. P. 10. Disponible en: https://docplayer.es/5875905-El-phishing-trabajo-final-de-grado-grado-en-criminologia-y-seguridad-alumno-mayra-sheila-mariana-leguizamon-tutor-manuel-mollar-villanueva.html

34. MEDINA RUVALCABA, Estefanía; San Martin, Cristos Velasco y Velázquez Olavarrieta, Andrés Recomendaciones para abordar la detección e investigación del fraude cibernético en México. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1057296/fraude_cibernetico.pdf

35. OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO. Compendio de Ciberdelincuencia Organizada, Viena, 2022. [en línea]. [consultado el 10 de abril de 2022]. Disponible en: https://www.unodc.org/documents/organized-crime/tools_and_publications/21-05345_S_eBook.pdf

36. Oficina de Naciones Unidas contra la Droga y el Delito UNODC, 2013, p. 72

37. Pereira Estupiñán, Francisco. La clonación de tarjetas de crédito en el Ecuador, ¿un delito económico? Ecuador, 2012. Disponible en: https://repositorio.uasb.edu.ec/bitstream/10644/3021/1/T1096-MDE-Pereira-La%20clonacion.pdf

38. Procuraduría Especializada Contra Crímenes y Delitos de Alta Tecnología. Procuraduría General de la República Dominicana [en línea]. [s.d] [consultado el 10 de mayo de 2022]. Disponible en: https://pgr.gob.do/pedatec/

39. QUEVEDO GONZÁLEZ, Josefina. *INVESTIGACION Y PRUEBA DEL CIBERDELITO*. Maestría, Universidad de Barcelona, 2017 [consultado el 16 de abril de 2021]. P.11. Disponible en: http://diposit.ub.edu/dspace/bitstream/2445/128112/1/JQG_TESIS.pdf

40. REPÚBLICA DOMINICANA. Congreso de la Republica Dominicana. Sobre Crímenes y Delitos de Alta Tecnología [en línea]. Ley n.º 53-07 de 23 de abril de 2007 [consultado el 10 de enero de 2022]. Disponible en: https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf

41. Reporte de ciberseguridad 2020 riesgos y avances y el camino a seguir en América Latina y el Caribe. Disponible en Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe (iadb.org)

42. REPÚBLICA DOMINICANA. Congreso de la Republica Dominicana. Sobre Crímenes y Delitos de Alta Tecnología [en línea]. Ley n.º 53-07 de 23 de abril de 2007 [consultado el 10 de enero de 2022]. Disponible en: https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf

43. REPÚBLICA DOMINICANA. Congreso de la Republica Dominicana. Sobre Propiedad Industrial [en línea]. Ley n.º 20-00 de 8 de mayo de 2000 [consultado el 10 de enero de 2022]. Disponible en: doi:file:///C:/Users/Usuario/Downloads/ley20-00.pdf

44. REPÚBLICA DOMINICANA. Congreso de la Republica Dominicana. Sobre Derecho de Autor [en línea]. Ley n.º 65-00 de 26 de julio de 2000 [consultado el

10 de enero de 2022]. Disponible en: https://www.aduanas.gob.do/media/2213/65-00_sobre_derecho_de_autor.pdf

45. Resolución AG/RES. 2004 (XXXIV-O/04) de 8 de junio de 2004 - Informática Jurídica. *Informática Jurídica* [en línea]. 28 de abril de 2021 [consultado el 10 de junio de 2022]. Disponible en: https://www.informatica-juridica.com/resolucion/resolucion-ag-res-2004-xxxiv-o-04-de-8-de-junio-de-2004/#:~:text=Resolución%20AG/RES.%202004%20(XXXIV-O/04)%20de%208%20de%20junio,una%20cultura%20de%20Seguridad%20Cibernética.%20AG/RES.%202004%20(XXXIV-O/04)

46. RINALDI, Paola. ¿De Dónde Viene El Delito Cibernético? Origen Y Evolución. *Le VPN Spanish* [en línea]. 27 de abril de 2017 [consultado el 9 de marzo de 2022]. Disponible en: https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/

47. ROMERO PÉREZ, Héctor Manuel. *Análisis de Los Crímenes y Delitos de Alta Tecnología en el Distrito Nacional, 2007-2013*. En: https://bibliotecaunapec.blob.core.windows.net/tesis/TPG_CI_MDP_48_2013_ET140182.pdf [base de datos en línea] [consultado el 15 de mayo de 2022]. Tesis de postgrado, Universidad APEC, 2013. Disponible en: https://bibliotecaunapec.blob.core.windows.net/tesis/TPG_CI_MDP_48_2013_ET140182.pdf

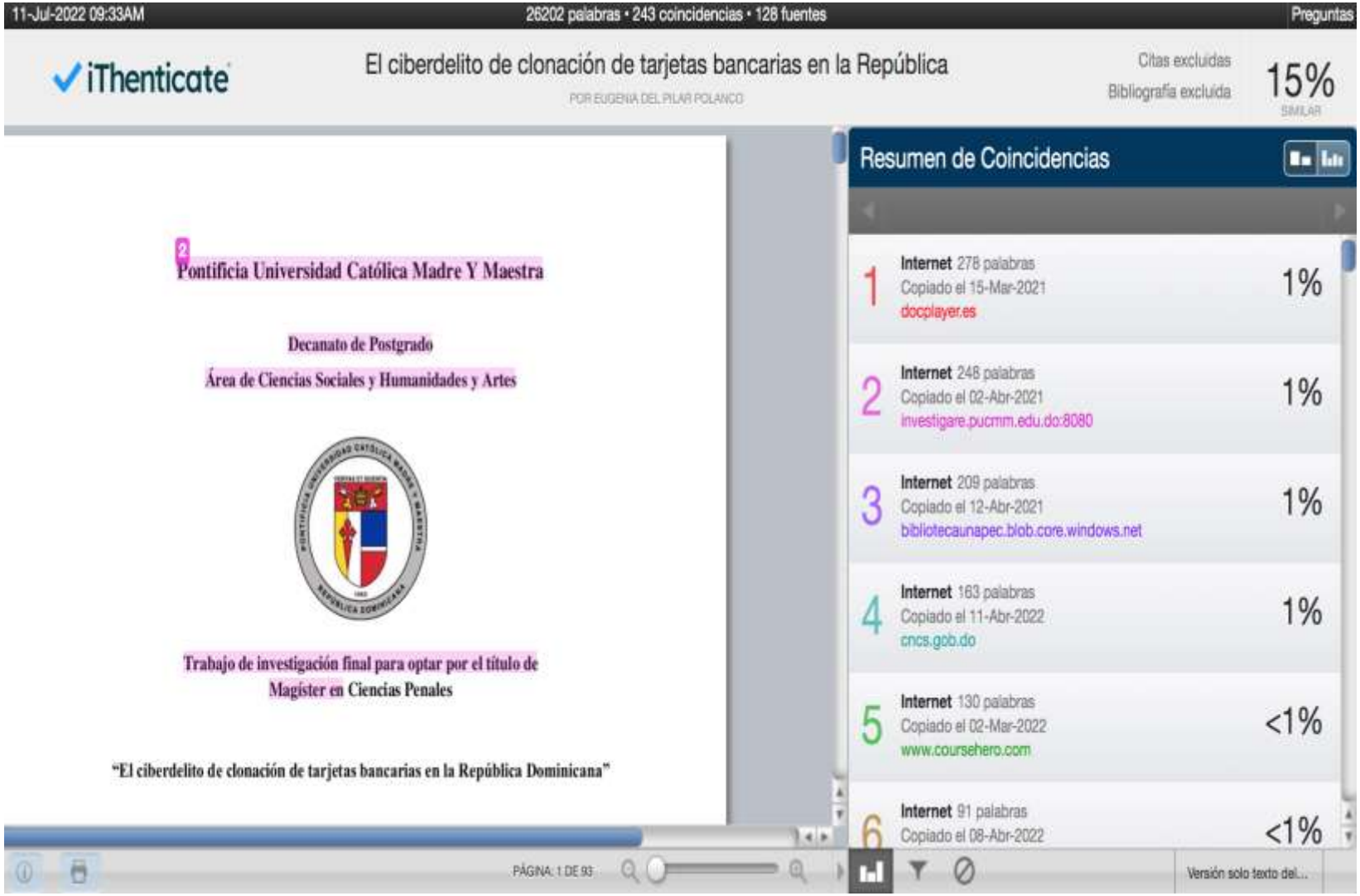
48. SANTOS LORENZO, Maritza. *Análisis de los medios probatorios idóneos para comprobar los delitos electrónicos en el Distrito Nacional, año 2019*. En: https://bibliotecaunapec.blob.core.windows.net/tesis/TPG_CI_MDP_06_2020_ET210180.pdf [base de datos en línea] [consultado el 15 de mayo de 2022]. Tesis de postgrado, Universidad APEC, 2020. Disponible en: https://bibliotecaunapec.blob.core.windows.net/tesis/TPG_CI_MDP_06_2020_ET210180.pdf

49. SERNAC (2022). Glosario para entender fraudes tecnológicos. Disponible en: https://www.sernac.cl/portal/607/w3-article-3259.html

50. SOSA PÉREZ, Rosalia**,** Comentarios al Derecho a la Intimidad y el Honor Personal, Constitución Comentada, Finjus, Segunda Edición, 2012, p. 110

51. TÉLLEZ VALDES, Julio. *DERECHO INFORMÁTICO* [en línea]. 2ª ed. Mexico: McGRAW-HILl/INTERAMERICANA DE MÉXICO, 1998. ISBN 970-10-0905-3 [consultado el 6 de marzo de 2021]. P. 187 -188.

Disponible
en: https://www.bing.com/search?q=TÉLLEZ+VALDÉS,+Julio,+2009.+Derecho+informático&cvid=6285287629f84a86813f8dd1e6ddd965&aqs=edge..69i57.982j0j4&FORM=ANAB01&PC=U531.


11-Jul-2022 09:33AM
26202 palabras • 243 coincidencias • 128 fuentes
Preguntas
iThenticate
El ciberdelito de clonación de tarjetas bancarias en la República
POR EUGENIA DEL PILAR POLANCO
Citas excluidas
Bibliografía excluida
15%
SIMILAR
Pontificia Universidad Católica Madre Y Maestra
Decanato de Postgrado
Área de Ciencias Sociales y Humanidades y Artes
Trabajo de investigación final para optar por el título de
Magíster en Ciencias Penales
"El ciberdelito de clonación de tarjetas bancarias en la República Dominicana"
Resumen de Coincidencias
1 Internet 278 palabras 1%
Copiado el 15-Mar-2021
docplayer.es
2 Internet 248 palabras 1%
Copiado el 02-Abr-2021
investigare.pucmm.edu.do:8080
3 Internet 209 palabras 1%
Copiado el 12-Abr-2021
bibliotecaunapec.blob.core.windows.net
4 Internet 163 palabras 1%
Copiado el 11-Abr-2022
cncs.gob.do
5 Internet 130 palabras <1%
Copiado el 02-Mar-2022
www.coursehero.com
6 Internet 91 palabras <1%
Copiado el 08-Abr-2022
PÁGINA: 1 DE 93
Versión solo texto del...

CITI PROGRAM

Completion Date 06-Jun-2022
Expiration Date 05-Jun-2024
Record ID 49390863

This is to certify that:

Eugenia del Pilar Polanco Disla

Has completed the following CITI Program course:

Not valid for renewal of certification through CME.

Human Subject Research Spanish
(Curriculum Group)
Curso de Ética en la Investigación para Estudiantes
(Course Learner Group)
1 - Basic Course
(Stage)

Under requirements set by:

Pontificia Universidad Católica Madre y Maestra (Santiago- República Dominicana)

CITI
Collaborative Institutional Training Initiative

Verify at www.citiprogram.org/verify/?w37ef18c6-9913-4f09-aaad-9a3a253c1ae4-49390863