Proyecto de Ley N°. 8854/2024-CR.

CONGRESO de la REPÚBLICA

HUAMÁN CORONADO RAÚL

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año del Bicentenario, de la consolidación de nuestra independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

CONGRESO DE LA REPÚBLICA
ÁREA DE TRÁMITE DOCUMENTARIO
09 SEP. 2024
RECIBIDO
Firma: Hora: 18:04 PM

LEY QUE DECLARA DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA IMPLEMENTACIÓN DE LOS ÓRGANOS JURISDICCIONALES ESPECIALIZADOS EN CIBERCRIMINALIDAD

El congresista que suscribe, **RAÚL HUAMÁN CORONADO**, integrante del **GRUPO PARLAMENTARIO FUERZA POPULAR**, en el ejercicio, del derecho de iniciativa legislativa que les confiere el artículo 107° de la Constitución Política del Perú y conforme lo establecen los artículos 22° inciso c), 67°, 75° y numeral 2 del artículo 76° del Reglamento del Congreso de la República, presenta el siguiente proyecto de ley:

FÓRMULA LEGAL:

El Congreso de la República

Ha dado la Ley Siguiente:

Firmado digitalmente por: INFANTES CASTAÑEDA Mery Eliana FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2024 17:37:30-0500

LEY QUE DECLARA DE INTERÉS NACIONAL Y NECESIDAD PÚBLICA LA IMPLEMENTACIÓN DE LOS ÓRGANOS JURISDICCIONALES ESPECIALIZADOS EN CIBERCRIMINALIDAD

ARTÍCULO ÚNICO. – DECLARATORIA

Declárese de interés nacional y necesidad pública la implementación de los órganos jurisdiccionales especializados en cibercriminalidad.

Dese cuenta
Lima, agosto de 2024

Firmado digitalmente por: SANTISTEBAN SUCLUPE Magally FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2024 17:55:57-0500

Firmado digitalmente por: HUAMAN CORONADO Raul FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 05/09/2024 17:06:17-0500

Firmado digitalmente por: OBANDO MORGAN Auristela Ana FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2024 17:08:49-0500

RAÚL HUAMÁN CORONADO
Congresista de la República
Documento firmado digitalmente

Firmado digitalmente por: ROSPIGLIOSI CAPURRO Fernando Miguel FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2024 16:30:01-0500

Firmado digitalmente por: VENTURA ANGEL Hector Jose FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2024 16:13:08-0500

Firmado digitalmente por: JIMENEZ HEREDIA David Julio FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2024 14:57:31-0500

Firmado digitalmente por: RAMIREZ GARCIA Tania Estefany FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2024 16:06:13-0500

Firmado digitalmente por: ALEGRIA GARCIA Luis Alberto FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 09/09/2024 16:20:00-0500

CONGRESO DE LA REPÚBLICA

Lima, **11** de **setiembre** de **2024**

Según la consulta realizada, de conformidad con el Artículo 77° del Reglamento del Congreso de la República: pase la Proposición **N° 8854/2024-CR** para su estudio y dictamen, a la (s) Comisión (es) de:

1. **JUSTICIA Y DERECHOS HUMANOS, y**
2. **DEFENSA NACIONAL, ORDEN INTERNO, DESARROLLO ALTERNATIVO Y LUCHA CONTRA LAS DROGAS.**

GIOVANNI FORNO FLOREZ
Oficial Mayor
CONGRESO DE LA REPÚBLICA

I. EXPOSICIÓN DE MOTIVOS

Ante la alarmante situación de los índices registrados de la cibercriminalidad los gobiernos han decidido implementar diferentes estrategias a fin de hacer frente estos fenómenos criminógenos producidos en el ciberespacio, mediante el uso de dispositivos y sistemas informáticos. Al respecto, en atención al avance de las tecnologías se han registrados ciberataques que han producido pérdidas económicas a empresas y organismos gubernamentales cada año causando graves daños patrimoniales con el pasar de los años.

En el caso peruano lamentablemente no hemos sido ajenos ante los ciberataques producidos por delincuentes que se han adaptado a esta nueva criminalidad mediante el uso de las nuevas tecnologías. En el país la cibercriminalidad ha agraviado tanto a personas naturales, como a personas jurídicas, entre ellas a empresas del sector privado como a organismos del Estado.

Con relación a empresas del sector privado, hemos advertido ciberataques realizados a importantes entidades bancarias, las cuales han afectado a la ciudadanía que ha pensado en el peligro de sus ahorros, ocasionándoles preocupaciones y desconfianza de estas entidades.

Respecto a los organismos estatales se han registrado intrusiones las cuales han puesto en peligro el servicio que brindan las autoridades por medio del ciberespacio, asimismo, se ha sufrido la exposición de información sensible por parte de las autoridades peruanas.

De este modo, en la actualidad tenemos un sistema de justicia que tiene un Ministerio Público y una policía con equipos y unidades especializadas en la investigación y persecución de la cibercriminalidad, sin embargo, no existe un circuito de jueces del Poder Judicial especializados en el procesamiento de este tipo de delitos, lo que confirma la necesidad de implementar órganos jurisdiccionales especializados en cibercriminalidad.

1. PROBLEMÁTICA

Con la finalidad de demostrar la necesidad de la implementación de los órganos jurisdiccionales especializados en cibercriminalidad, es importante revisar los índices delitos respecto a los delitos informáticos.

De esta manera, conforme a los datos de la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (DIVINDAT), quienes están encargados de investigar, denunciar y combatir el crimen organizado transnacional, en el ámbito de delitos que se comentan mediante el uso de la tecnología de información y comunicación, podemos conocer la cantidad de denuncias presentadas respecto a delitos informáticos.

Es importante revisar el siguiente cuadro adaptado del informe N° 237-2020-DIRINCRI-PNP/DIVINDAT-SEC, de fecha 14 de septiembre de 2020 y de información remitida por el Coronel Orlando Mendieta, jefe de DIVINDAT, a la OFAEC de fecha 20 de enero de 2021, obtenido del ***Informe de Análisis N° 04 – Ciberdelincuencia en el Perú: Pautas para una Investigación Fiscal Especializada***, elaborado por la Oficina de Análisis Estratégico contra la Criminalidad-OFAEC de la Fiscalía de la Nación, el cual compartimos a continuación.

CUADRO N°1

Denuncias de delitos informáticos investigados por la DIVINDAT 2013-2020[1]

Delito	2013	2014	2015	2016	2017	2018	2019	2020	Total	%
Abuso de mecanismo y dispositivos informáticos	**14**	**3**	**6**	**4**	**5**	**1**	**2**	**19**	**54**	**0.4%**
Suplantación de identidad	**10**	**101**	**114**	**134**	**132**	**227**	**247**	**572**	**1537**	**12.6%**
Suplantación de identidad	10	101	114	134	132	227	247	568	1533	
Suplantación de identidad virtual								4	4	
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	**9**	**9**			**29**	**94**	**49**	**100**	**290**	**2.4%**
Contra la indemnidad sexual de menores								2	2	
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	9	9			29	94	49	98	288	
Contra datos y sistemas informáticos	**38**	**62**	**47**	**47**	**104**	**126**	**159**	**177**	**760**	**6.2%**
Acceso ilícito	11	42	1	1	49	84	129	151	468	
Acceso ilícito a una base de datos								2	2	
Atentado a integridad de datos informáticos	21	4	30	22	40	26	5	9	157	
Atentado a la integridad de sistemas informáticos	6	16	16	24	15	9	5	9	100	
Atentado contra la integridad de datos y sistemas informáticos						7	20	6	33	
Contra la intimidad y el secreto de las comunicaciones						**3**	**2**	**8**	**13**	**0.1%**
Interceptación de datos								2	2	
Interceptación de datos personales								1	1	
Tráfico ilegal de datos						3	2	5	10	
Fraude informático	**298**	**334**	**414**	**610**	**1219**	**1928**	**2097**	**2615**	**9515**	**78.2%**
Clonación de tarjeta	83	42	46	44	30	120	25	4	394	4
Compras fraudulentas por internet						287	431	261	979	10
Operaciones y transferencia electrónicas y/o de fondos no autorizados	215	292	368	566	1189	1521	1641	2350	8142	86
TOTAL	**369**	**509**	**581**	**795**	**1489**	**2379**	**2556**	**3491**	**12169**	**100.0%**

[1] Ministerio Público – Fiscalía de la Nación. (2021). Informe de Análisis N° 04 – Ciberdelincuencia en el Perú: Pautas para una Investigación Fiscal Especializada. Pg 20. Recuperado el 4 de octubre de 2022 de: https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf

De lo expuesto en el cuadro anterior, podemos ver que, en el periodo de octubre 2013 a diciembre de 2020, se registraron 12169 delitos vinculados a la Ley 30096 denunciados. El 78% (9515) de los delitos registrados es por fraude informático, seguido por el delito de suplantación de identidad (13%) y delitos contra datos y sistemas informáticos (6%).

Asimismo, podemos observar que, según las denuncias de delitos informáticos investigados por la DIVINDAT de 2013 a 2020, en el año 2013 se registraron 369 delitos, en el 2014 se registraron 509 delitos, para el 2015 se registraron 581 delitos, para el 2016 se registraron 795 delitos, para el 2017 se registraron 1489 delitos, para el 2018 se registraron 2379, para el 2019 se registraron 2556 delitos y para el 2020 se registraron 3491 delitos.

Respecto al año 2021, se tiene que entre enero y abril se investigaron 1188 denuncias de delitos cibernéticos en la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía. Los casos más frecuentes están relacionados al fraude informático y a la suplantación de identidad. Además, el coronel PNP Erick Ángeles, jefe de la DIVINDAT, explicó a la agencia Andina que los ciberdelincuentes recurren al email masivo, las redes sociales, sitios web falsos y mensajes de texto para estos ciberdelitos. Cada mes se estima que se reciben 300 denuncias por ciberdelitos[2].

La siguiente información ha sido recogida por la Oficina de Racionalización y Estadística del Ministerio Público respecto a las denuncias por delitos informáticos (Ley N°30096), registradas en el Sistema de Gestión Fiscal (SGF) y el Sistema Integrado de Apoyo al Trabajo Fiscal (SIATF), desde el 22 de octubre de 2013 al 31 de julio de 2020.

De este modo, resulta importante revisar el siguiente cuadro adaptado del reporte de la Oficina de Racionalización y Estadística, remitido a la OFAEC a través de correo electrónico de fecha 18 de agosto de 2020, obtenido del ***Informe de Análisis N° 04 – Ciberdelincuencia en el Perú: Pautas para una Investigación Fiscal Especializada***, elaborado por la Oficina de Análisis Estratégico contra la Criminalidad-OFAEC de la Fiscalía de la Nación, el cual compartimos a continuación.

En atención a la información recogida por el Ministerio Público, se observa que anualmente las denuncias muestran incrementos constantes. Es así que, en el año 2014 se registraron 540 denuncias y en el año 2015 éstas llegaron a 907. En el año 2016 se elevaron a 1410 y un año después se duplicaron hasta alcanzar las 2841 denuncias. En el año 2018, las denuncias continuaron ascendiendo hasta llegar a 4648 y cerrar el año 2019 con 8504 denuncias, representando este último año el 39% de todas las denuncias ingresadas, entre los años 2014 y 2019.

CUADRO N°2

[2] Redacción El Peruano (02 de junio de 2021). Ciberdelitos en el Perú: se elevan denuncias de fraude informático y suplantación de identidad - Cada mes se registran cerca de 300 denuncias de delitos informáticos en promedio en la Divindat. Diario El Peruano. Recuperado el 4 de octubre de 2022 de: https://elperuano.pe/noticia/121876-ciberdelitos-en-el-peru-se-elevan-denuncias-de-fraude-informatico-y-suplantacion-de-identidad

Denuncias por delitos informáticos registradas en Fiscalías Penales Comunes y Fiscalías Mixtas, de octubre 2013 a julio 2020[3]

Ciudad	2013	2014	2015	2016	2017	2018	2019	2020	Total	%
Lima	67	325	550	708	1495	2366	3713	1116	10340	47.68%
Lima Norte	3	24	24	99	174	357	717	220	1618	7.46%
Arequipa	1	18	47	155	255	291	506	115	1388	6.40%
Lima Este	3	17	26	53	147	251	603	183	1283	5.92%
La Libertad	3	20	35	36	94	213	487	232	1120	5.16%
Lambayeque	1	11	31	82	119	182	326	124	876	4.04%
Callao	3	15	16	52	57	130	322	101	696	3.21%
Lima Sur	1	4	9	27	52	120	355	119	687	3.17%
Cusco	4	33	42	41	79	81	176	81	537	2.48%
Ica		3	10	22	24	91	195	57	402	1.85%
Piura	3	10	33	15	34	68	134	40	337	1.55%
Loreto	1	7	15	24	48	93	100	32	320	1.48
Moquegua	1	2	1	5	19	46	141	47	262	1.21%
Santa		3	3	6	36	20	90	27	185	0.85%
Huánuco		3	2	3	30	25	61	36	160	0.74%
Junín		5	7	5	16	44	52	27	156	0.72%
Ucayali		4	6	9	18	43	44	15	139	0.64%
San Martin		3	4	6	32	31	49	13	138	0.64%
Amazonas	2	1	2	6	30	18	51	20	130	0.60%
Cajamarca	1	3	2	4	5	21	59	31	126	0.58%
Ayacucho	2	3	2	9	9	24	50	15	114	0.53%
Tacna		6		5	4	20	50	15	100	0.45%
Sullana		3	12	9	12	15	25	15	91	0.42%
Huaura		4	6	8	11	20	32	10	91	0.42%
Ancash		2	4	5	12	20	35	8	86	0.42%
Lima Noroeste			2	6	3	15	31	15	72	0.33%
Puno	1		3	3	12	8	15	6	48	0.22%
Apurímac		3	1	1	2	18	13	4	42	0.19%
Madre de Dios		2	3		3	1	23		32	0.15%
Tumbes		4	3	2	5	6	8	1	29	0.13%
Huancavelica	1	1	2	3		4	17	1	29	0.13%
Cañete		1	1	1	1	15	3	3	23	011%
Selva Central			3		1	1	5	8	28	0.08%
Paco	1				2	4	4	1	12	0.06%
TOTAL	**99**	**540**	**907**	**1410**	**2841**	**4648**	**8504**	**2738**	**21687**	**100.0%**

[3] Ministerio Público – Fiscalía de la Nación. (2021). Informe de Análisis N° 04 – Ciberdelincuencia en el Perú: Pautas para una Investigación Fiscal Especializada. Pg 22. Recuperado el 4 de octubre de 2022 de: https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf

Respecto al año 2021, se tiene que, según datos del Ministerio Público, se recibieron 18 mil 596 denuncias de casos de cibercrimen, lo que representa un incremento porcentual de 92,9% en comparación con el año 2020[4].

Conforme a los datos expuestos provenientes de la Policía Nacional del Perú, Ministerio Público, Poder Judicial, Ministerio de Justicia y Derechos Humanos y Defensoría del Pueblo, podemos observar que los índices de la ciberdelincuencia vienen aumentando año tras año. Esto generaría muchos problemas respecto a la afectación de la seguridad ciudadana, así como la sobrecarga procesal del Sistema Penal. Por otro lado, realizando una comparación frente a los datos expuestos, en atención a las estadísticas de la Oficina de Control de la Productividad Fiscal (OCPF) de la Base de datos del Sistema de Gestión Fiscal (SGF) y el Sistema de Información de Apoyo al Trabajo Fiscal (SIATF) del Ministerio Público, podemos observar que existe una gran cantidad de delitos informáticos archivados por diferentes motivos. Lo referido es preocupante, por cuanto se estaría generando lo que se conoce como el paraíso de la impunidad. En atención ello, nos lleva a realizar la siguiente pregunta *¿Qué deben hacer los organismos que componen el Sistema Penal peruano frente a los índices de cibercriminalidad y los índices de impunidad?*

Respecto al ***Diagnóstico Situacional Multisectorial sobre la Ciberdelincuencia en el Perú*** publicado por el Ministerio de Justicia y Derechos Humanos, podemos observar que las medidas implementadas en el Perú no han sido suficientes para la lucha contra la cibercriminalidad.

En la actualidad no existe una Ley en Ciberseguridad en el Perú que pueda sentar las bases en materia de ciberseguridad. Tampoco se ha implementado una política o Plan gubernamental materia de ciberseguridad o contra la ciberdelincuencia. Esto es grave por cuanto en otros países de la región, como Argentina, Chile, Colombia o Ecuador, cuentan con estas medidas implementadas a fin brindar seguridad de las personas en el ciberespacio.

De igual forma, por parte de las instituciones que componen el Sistema Penal, podemos señalar que no existen protocolos institucionales o interinstitucionales para el tratamiento de la ciberdelincuencia. Asimismo, tampoco existe una estrategia de coordinación entre el Poder Judicial, Ministerio Público y la Policía Nacional del Perú. Solamente la Policía Nacional del Perú y el Ministerio Público, han implementado organismos especializados para el tratamiento de la cibercriminalidad. Sin embargo, a pesar de los esfuerzos de las instituciones mencionadas, el Poder Judicial no ha implementado estrategias o órganos especializados frente a la cibercriminalidad.

---

[4] Redacción El Peruano (04 de septiembre de 2022). Denuncias por delitos informáticos se incrementaron en más del 90% en el Perú. Diario El Peruano. Recuperado el 4 de octubre de 2022 de: https://www.elperuano.pe/noticia/188048-denuncias-por-delitos-informaticos-se-incrementaron-en-mas-del-90-en-el-peru#:~:text=Seg%C3%BAn%20datos%20del%20Ministerio%20P%C3%BAblico,en%20comparaci%C3%B3n%20con%20el%202020.

Aunado a ello, en el Informe de Análisis N° 04 – Ciberdelincuencia en el Perú: Pautas para una Investigación Fiscal Especializada, con el objetivo de conocer la experiencia, percepción y opinión de los fiscales en la investigación de los delitos informáticos, se diseñó un cuestionario de 21 preguntas, el mismo que fue aplicado por vía correo electrónico y la plataforma Google Forms a 8 Fiscales de las Fiscalías Provinciales Penales de mayor incidencia de denuncias por delitos informáticos en el periodo de octubre 2013 a julio 2020[5].

En la referida muestra realizada a los 8 Fiscales de las Fiscalías Provinciales, indicaron que tuvieron dificultades en la investigación y enjuiciamiento en la ciberdelincuencia. Respecto a las diligencias preliminares, se indica que tuvieron dificultades relacionadas al identificar al autor y poca información, los jueces se niegan el levantamiento del secreto a las telecomunicaciones (art. 230 del NCPP), así como necesidad de equipos de alta tecnología para identificar autores. También se indicó como dificultades los insuficientes o deficientes órganos de apoyo. Se precisa que la referida dificultad consistió en la falta de capacitación de los policías en uso de técnicas de investigación especial y falta de peritos en la materia.

Respecto a la etapa de formalización y continuación de la investigación preparatoria, se indicó que tuvieron problemas por cuanto la falta de capacidades tecnológicas de la Policía Nacional del Perú, falta de peritos y en la cooperación con otras Fiscalías para investigar imputados que se encuentran fuera del Distrito Fiscal. En la etapa de juicio oral, los fiscales indicaron que tuvieron problemas respecto a la poca asistencia de los peritos al juicio oral y a la ubicación de los órganos de prueba, agraviado y efectivos policiales para la participación en el proceso.

Conforme a lo recogido del Informe de ***Análisis N° 04 – Ciberdelincuencia en el Perú: Pautas para una Investigación Fiscal Especializada***, entendemos que la referida encuesta fue realizada a fiscales de 8 fiscalías, sin embargo, esto nos es útil a fin de estudiar la problemática en la investigación y procesamiento de la ciberdelincuencia.

En atención a los datos expuestos por parte de las entidades públicas encargadas de la persecución penal y procesamiento de los delitos informáticos, resulta evidente la necesidad de implementar acciones preventivas para la persecución y sanción de los ciberdelitos.

Conforme a la base de datos del Registro Nacional de Condenas, elaborado por la Sub-Gerencia de Estadística – Gerencia de Planificación del Poder Judicial, podemos conocer la cantidad de personas con sentencia registrada según delitos informáticos y contra el patrimonio relavo al delito informático. En tal sentido compartimos el siguiente cuadro, que hemos adaptado en atención a la información obtenida del Poder Judicial:

[5] Ministerio Público – Fiscalía de la Nación. Op.cit. Pg. 35-42

CUADRO N°3

Personas con sentencia condenatoria registrada según delitos informáticos y contra el patrimonio relativo a delito informático – Periodo 2016 – 2020[6].

Delito	Años					
	2016	2017	2018	2019	2020[7]	Total
Delitos Informáticos (Ley 30096 y 30171)	**33**	**25**	**142**	**149**	**43**	**392**
Acceso Ilícito – Art. 2 – Ley N° 30096		2	1	4		7
Atentado a la Integridad de Datos Informáticos – Art. 3 - Ley N° 30096			4	1	1	6
Atentado a la Integridad de Sistemas Informáticos – Art. 4 - Ley N° 30096		1	1			2
Fraude Informático – Art. 8 - Ley N° 30096	21	9	94	118	30	272
Interceptación de datos informáticos	1	2	2	3	1	9
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos – Art. 5 - Ley N° 30096	8	11	34	23	11	87
Suplantación de Identidad – Art. 9 - Ley N° 30096	3		6			9
Título V Delitos Contra el Patrimonio (Artículo 185 al 208)						
Delitos Informáticos (Artículo 207-A al 207-D)	4	36	3	3	2	48
Alteración, Daño o destrucción de base de datos Art. 207-D				3	2	5
Delito Informático – Art. 207-C Agravantes		1	2			3
Delito Informático Art. 207		34				34
Tráfico Ilegal de datos – Art. 207 - Ley N° 30096	1					1
Uso o Ingreso indebido a una base de datos Art. 207-A	3	1	1			5
Total	**37**	**61**	**145**	**152**	**45**	**440**

[6] Cuadro adaptado de la información brindada de la base de datos del Registro Nacional de Condenas, elaborado por la Sub Gerencia de Estadística – Gerencia de Planificación del Poder Judicial.

[7] Incluye datos registrados hasta el 29 de octubre de 2020.

Al respecto, según la información del Poder Judicial, se tiene que el año 2016 se condenaron a 37 personas, en el año 2017 se condenaron a 61 personas, en el año 2018 se condenaron a 145 personas, en el año 2019 se condenaron a 152 personas y hasta octubre del año 2020 se condenaron a 45 personas. De este modo, desde el año 2016 hasta octubre del año 2020, se registraron un total de 440 sentencias condenatorias.

2. LA ESPECIALIZACIÓN DE LOS ÓRGANOS JURISDICCIONALES

La especialización de la jurisdicción ha sido implementada por los sistemas de justicia con la finalidad de atender diversas situaciones que requerían una intervención diferente a la ordinaria.

Con relación a las jurisdicciones especiales, Echandía sostiene que inicialmente fueron los mismos jueces quienes se les encomendó la administración de justicia en toda clase de casos y materias, sin embargo, debido a la complejidad de las relaciones sociales obligó a diversificar el derecho sustancial que debía armonizarlas, y así fue con aparecieron la rama del derecho civil y la penal y luego, aparecieron más ramas[8].

Por su parte, Véscovi sostiene que las jurisdicciones especiales se tratan de magistraturas especializadas para efectuar el mismo proceso, con ciertas especialidades[9].

Respecto a la definición de la jurisdicción ordinaria, especial y extraordinaria Ovalle Favela señala lo siguiente:

> *"(...) se suele entender por jurisdicción ordinaria o común la que ejercen los juzgadores que tienen competencia para conocer la generalidad de los litigios; por jurisdicción especial la que compete a los juzgadores para conocer la cierta clase de litigios, y por jurisdicción extraordinaria la que se atribuye a órganos creados ex proceso para conocer de uno o más litigios concretos y determinados[10]."*

Aunado a ello, sobre la jurisdicción especializada Fix-Fierro sostiene lo siguiente:

> *"Dada la tendencia general en la sociedad hacia una mayor división y especialización del trabajo, se puede decir con certidumbre que este solo hecho requeriría una tendencia equivalente en la administración de justicia[11]."*

---

[8] Echandía, H. D. (1984) Teoría General del Proceso. Tomo I. Editorial Universidad. Pg. 58.
[9] Véscovi, E. (1999) Teoría General del Proceso. Editorial Temis. Pg. 105.
[10] Ovalle Favela, J. (2016) Teoría General del Proceso. Oxford University Press. PP. 144-145.
[11] Fix-Fierro, H. (2013) Tribunales, Justicia y Eficiencia. Estudio sociojurídico sobre la racionalidad económica en la función judicial. Universidad Nacional Autónoma de México. Pg. 299.

En atención a lo expuesto por los citados autores, podemos colegir que la creación de jurisdicciones especiales obedece a la necesidad de atender materias o casos específicos que requieren una atención diferenciada o especializada con la finalidad de brindar un servicio eficiente y eficaz del sistema de justicia.

Asimismo, el mencionado Fix-Fierro citando a Legomsky menciona los criterios que favorecen la especialización, los cuales compartimos a continuación:

- *"Mezcla de derecho, hechos, y facultades discrecionales: el predominio de resoluciones discrecionales y de cuestiones de hecho en la etapa de audiencia inicial favorecen usualmente la especialización.*
- *Complejidad técnica.*
- *Grado de aislamiento: lo que significa, por un lado, que las cuestiones jurídicas en un área pueden resolverse ordinariamente sin referencia a la resolución de problemas en otras áreas; y por el otro, que las analogías hacia cuestiones externas al área son relativamente infrecuentes.*
- *Cohesión: alto grado de interrelaciones dentro de una sola materia.*
- *Grado de repetición: alto número de asuntos similares y necesidad de consistencia en su resolución.*
- *Grado de controversia.*
- *"Tribalidad": la existencia de un grupo cerrado de abogados, funcionarios de gobierno, peritos, etcétera.*
- *Importancia particular de la consistencia: tanto en términos de igualdad como de política jurídica.*
- *Dinamismo: material sujeto a rápidos cambios.*
- *Logística: volumen, tiempo requerido por cada asunto, distribución geográfica.*
- *Necesidad particular de rápida resolución.*
- *Requerimientos procesales especiales*[12]*."*

Asimismo, respecto a las ventajas de la especialización de los órganos jurisdiccionales los autores Pascual y Mora-Sanguinetti [13] exponen las siguientes:

a) Reducción de los costes marginales de la resolución de asuntos

Los autores señalan que la especialización de la judicial conllevaría a la reducción del tiempo que necesitan para la resolución de los casos, por cuanto se reduce la cantidad de casos que se avocarán y los conocimientos adquiridos que le permitirán desarrollar los casos con mayor facilidad.

[12] Fix-Fierro, H. Op.cit. Pg. 301-302

[13] Pascual, D. y Mora-Sanguinetti, J. S. (2015) El mito de la especialización judicial. Indret. Revista para el Análisis del Derecho Núm. 1 Pág. 16-33. Recuperado el 23 de noviembre de 2023 de: https://raco.cat/index.php/InDret/article/view/293052

En atención a ello, los mencionados autores Pascual y Mora-Sanguinetti, sobre la reducción de los costes marginales de la resolución de asuntos señalaron lo siguiente:

> *"Pues bien, la especialización, ya lo hemos visto, reduce la variedad de los asuntos de los que un juez ha de conocer. Incrementa sus semejanzas y minora sus diferencias. Ello propicia que aumente la probabilidad y la medida en que los conocimientos aprendidos en la resolución de un caso pueden luego servir para decidir sobre otros. Hace que el tiempo y el esfuerzo requeridos para juzgar un caso adicional tiendan a disminuir o, dicho con otras palabras, que el coste marginal de producir una nueva resolución judicial decrezca, al menos hasta cierto punto[14]."*

b) Posibilidad de acortar la duración de los procedimientos, incrementar el número de asuntos resueltos y mejorar el acierto y la calidad de las decisiones judiciales

Aunado a ello, también se señala que la especialización judicial contribuye a tener jueces con mayor experiencia en un determinado tema, lo implica que en cada caso los jueces tienen mayores conocimientos para dar por terminado un proceso en menos tiempo que le tomaría una causa la cual no está acostumbrado o no tiene la experiencia del día a día.

Sobre la eficiencia como ventaja de la especialización de los órganos jurisdiccionales, Álvarez, citando a Fix-Fierro y a Legomsky expone lo siguiente:

> *"la eficiencia puede ser: para reducir la carga de los tribunales generales; porque los jueces poseen conocimientos lo que permite dedicar más tiempo a problemas específicos; porque menos jueces se dedicarán a la misma cuestión con lo cual se disminuye la posibilidad de contradicción; y al evitar conflictos sobre la competencia de los tribunales, entre otros" (Legomsky, 1990, citado en Fix- Fierro, 2013).*
>
> *La experiencia de los jueces hace que puedan identificar con mayor rapidez las cuestiones relevantes de los juicios (Ginsburg y Wright, 2013), lo cual coincide con lo expuesto por Legomsky en cuanto al menor tiempo para "educar" a jueces. En las experiencias de los actores relevantes de los Tribunales de Competencia y Telecom algunos destacaron precisamente que se redujo la duración de los litigios y que se fue acumulando conocimiento "(Álvarez, 2020)*[15].

[14] Pascual, D. y Mora-Sanguinetti, J. S. Op.cit. Pg. 10.
[15] Álvarez, C. L. (2021). Tribunales especializados en competencia y telecomunicaciones: por qué, para qué y cómo. Cuestiones constitucionales, (45), 3-46. Epub 09 de mayo de 2022.https://doi.org/10.22201/iij.24484881e.2021.45.16656

c) Uniformidad

También se señala que la uniformidad como una ventaja a la especialización judicial por cuanto se señala que, en un ámbito determinado o un circuito de órganos jurisdiccionales, se reducirán las posibilidades de pronunciamientos distintos debido a la práctica judicial y la cercanía de los jueces.

Asimismo, Pascual y Mora-Sanguinetti sobre la uniformidad y coherencia interna señalaron lo siguiente:

> *"Al minorar la cantidad de órganos jurisdiccionales competentes para juzgar sobre una determinada materia, la especialización mitiga el riesgo de que en ese ámbito se dicten decisiones contradictorias o incoherentes, lo cual redunda en beneficio de la seguridad jurídica e igualdad de los justiciables, y evita allí los conflictos y las disfunciones que las contradicciones e inconsistencias jurisprudenciales suelen provocar[16]".*

d) Legitimidad

Se señala que la especialización de los órganos jurisdiccionales conlleva a una mayor legitimidad de estos, por cuanto, conforme a obtener resultados eficaces y eficientes en mucho menos tiempo que la jurisdicción ordinaria, esto significaría una reducción de la sensación de impunidad frente a la sociedad.

Como un ejemplo de esta ventaja, podemos citar el caso peruano de los jugados de flagrancia, los cuales, mediante la aplicación del proceso inmediato, han obtenido buenos resultados, lo que ha llevado a las autoridades peruanas a seguir implementado estos órganos especializados a fin continuar con más resultados positivos y de esta forma obtener una mayor legitimidad.

3. LOS ÓRGANOS JURISDICCIONALES ESPECIALIZADOS EN CIBERCRIMINALIDAD COMO POLÍTICA CRIMINAL

La implementación de los órganos jurisdiccionales especializados en el tratamiento del cibercrimen va de la mano con una idónea política criminal eficientemente elaborada para el tratamiento de la cibercriminalidad. En tal sentido corresponde el desarrollo de las bases de la Política Criminal y su relación con el cibercrimen, a fin de fundamentar los órganos jurisdiccionales especiales en el cibercrimen.

Sobre la Política Criminal Jescheck señala que conecta con las causas del delito, se ocupa de cómo hayan de recogerse correctamente los elementos de los tipos penales para responder a la realidad de aquél, intenta determinar los efectos de las sanciones empleadas en el derecho penal, considera hasta que

[16] Pascual, D. y Mora-Sanguinetti, J. S. Op.cit. Pg. 12.

límite puede extender el legislador el derecho penal para no restringir la espera de libertad del ciudadano[17].

Por su parte, Peña Cabrera Freyre comenta que la Política Criminal es aquella ciencia política social, que se orienta y encamina a formular positivamente una lucha adecuada y eficaz contra la criminalidad, de arreglo con el principio de legalidad y de las instituciones encargadas funcionalmente a ejecutarla[18].

Asimismo, Borja Jiménez define a la Política Criminal como aquel sector del conocimiento que tiene como objeto el estudio del conjunto de medidas, criterio y argumentos que emplean los poderes públicos para prevenir y reaccionar freten al fenómeno criminal.[19]

Al respecto, la profesora Laura Zúñiga Rodríguez señala que la política criminal debe elaborarse en base a estudios científicos para entender las aristas de la problemática social[20].

En atención a lo expuesto, resulta idóneo utilizar los instrumentos que brinda los diferentes campos de la ciencia para el desarrollo de la política criminal, más aún, si se pretende utilizar la política criminal para el tratamiento del fenómeno criminal relacionado a las modernas tecnologías.

Sobre el avance de la tecnología frente a la seguridad en el ciberespacio, Nayia Barmpaliou, Jefa de Políticas e Iniciativas Públicas del Centro para la Ciberseguridad del Foro Económico Mundial, señala lo siguiente:

> "*el desequilibrio entre el tiempo de comercialización y el "tiempo de seguridad" sigue siendo una cuestión predominante, debido a la presión de las fuerzas del mercado en favor de los productos de nuevas tecnologías, sin incentivos para priorizar los elementos de seguridad desde el inicio del ciclo de vida del producto*" [21].

En atención con lo expresado por la referida autora, podemos entender que la evolución de la tecnología avanza a un nivel más rápido que del desarrollo de la seguridad aplicada a los riesgos que pueden ocasionar estas tecnologías. Es de esta forma que, cuando los riesgos en el ciberespacio no pueden ser controlados mediante mecanismos no punitivos, resulta necesario la aplicación de la Política Criminal para el tratamiento de estos fenómenos criminales, así como para establecer su prevención.

---

[17] Jesheck, H. (1993). Tratado de Derecho Penal Parte General. 4ta edición. Editorial Comares – Granada. Pg. 18.
[18] Peña Cabrera Freyre, A. L. Op.cit. Pg 38.
[19] Borja Jiménez, E. (2011). Curso de Política Criminal. 2da Edición. Tirant Lo Blanch. Pg. 21.
[20] Zúñiga Rodríguez, L. Op.cit. Pp. 47-48.
[21] Barmpaliou, N. (2020). Amenazas emergentes en ciberseguridad: implicaciones para América Latina y el Caribe. En Porrúa, M. (coordinador). Ciberseguridad Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe – Reporte Ciberseguridad 2020. OAS y BID. Pg. 28. Recuperado el 14 de abril de 2023 de: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Así, en el caso de Política Criminal y su implicancia en el cibercrimen, consideramos que uno de los primeros desafíos a enfrentar fue que las legislaciones estaban dirigidas para la prevención, investigación y procesamiento del fenómeno criminal en el espacio físico. Por lo que, con la aparición de nuevas tecnologías que han traído consigo nuevas formas de vulneración de bienes jurídicos, en un ámbito no físico conocido como el ciberespacio, esto ha obligado a los Estados a actualizar sus normativas a fin de lograr la protección de sus ciudadanos.

Sobre este punto, el profesor Claus Roxin señala que en ninguna parte se ha logrado eliminar la criminalidad, ni siquiera alcanzar su marginación; tampoco existe un acuerdo sobre el camino razonable para reducirla, concluyendo que las tendencias de la política criminal cambian como la moda[22].

En tal sentido, así como la tecnología y su implicancia en el fenómeno criminal está en constante evolución, de igual forma la política criminal debe adaptarse a las situaciones actuales con la finalidad que el Estado brinde un eficaz tratamiento frente a las nuevas formas de criminalidad.

De este modo la profesora Zúñiga Rodríguez sostiene que la criminalidad es producto de la Sociedad, la cual crea nuevas formas de criminalidad a las que la Política Criminal tiene que hacer frente[23].

Al respecto, en las resoluciones XIX Congreso Internacional de Derecho Penal, de la Asociación Internacional de Derecho Penal, celebrado en Río de Janeiro entre el 31 de agosto y 6 de septiembre de 2014, con el nombre de Sociedad de la Información y Derecho Penal, consideraciones sobre la política criminal respecto a la protección de redes de las Tecnologías de la Información y comunicación, señalándose también que la Política Criminal debe ser coherente con los principios de la legislación penal. De igual forma, en el referido congreso se hace mención de la necesidad de la actualización de la legislación penal y procesal penal. Asimismo, se establece que se deben armonizar a nivel mundial las políticas relacionadas con la protección de las redes TIC y el ciberespacio y los intereses de los usuarios, con el fin de evitar graves discrepancias entre las regulaciones de la misma materia, mejorar la cooperación internacional y evitar conflictos de jurisdicción.

Por su lado, el profesor Borja Jiménez comenta que la política criminal de lucha contra la delincuencia informática debe ir encaminada, en primer lugar, a crear una legislación penal sustantiva y procesal que puede desarrollarse en un conjunto importante de Estados seriamente implicados en esta actividad de hacer frente a dicha criminalidad[24].

---

[22] Roxin, C. (2002). Problemas actuales de la Política Criminal. En Díaz Aranda, E. (Editor). Problemas Fundamentales de la Política Criminal y Derecho Penal. Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México. Pp. 87-88.
[23] Zúñiga Rodríguez, L. Op.cit. Pg. 252.
[24] Borja Jiménez, E. Op.cit. Pg. 292.

Además, sobre la prevención de los ataques a los sistemas informáticos, Mata y Martín señala que exigen la adopción planificada de un conjunto de medidas de seguridad previo un análisis de las necesidades de protección específicas y de las hipotéticas fuentes de peligro[25].

Sobre la prevención de los ciberataques en la Política Criminal, esto también fue mencionado en las resoluciones del XV Congreso Internacional de Derecho Penal, el cual se realizó entre el 4 al 10 de septiembre de 1994, en Río de Janeiro. Al respecto, en la Sección II: Infracciones informáticos y otros delitos contra a tecnología informática se establecieron como recomendaciones establecer medidas de prevención no penales para evitar el delito informático.

En esa misma línea, el profesor Vidaurri Aréchiga sostiene que la Política criminal no se agota en la utilización casi exclusiva del Derecho penal; por el contrario, es clara la posibilidad y conveniencia de valerse de otro tipo de medidas que puedan enfrentar la criminalidad de manera menos intensa que la penal y, probablemente, sean hasta más efectivas[26].

Conforme a lo expuesto, la prevención de los ciberdelitos desde el ámbito no penal, debe ser una parte fundamental en una política criminal para el tratamiento de la cibercriminalidad. De este modo varios autores han señalado que la mejor Política Criminal, es una correcta Política Social o Política General, por cuanto en estas se establecen medidas para la prevención de ciberataques, como medidas de ámbitos educativos, sociales, económicos, regulatorios o culturales[27].

Sin embargo, en algunas situaciones podemos utilizar las herramientas preventivas que nos brinda el derecho procesal, más aún cuando estamos ante situaciones críticas, donde estamos expuestos ante una importante cantidad de ciberataques, los cuales han demostrado que pueden ocasionar graves afectaciones, no solo a la ciudadanía en forma individualizada, sino también pueden causar graves daños instituciones públicas y privadas, y de esta forma afectar a miles de personas.

Asimismo, otro tema importante a tener en consideración por parte de la Política Criminal, se encuentra relacionada a la transnacionalidad del cibercrimen. En ese sentido deberá desarrollarse los mecanismos de cooperación judicial internacional para la persecución y procesamiento de la cibercriminalidad.

En atención a ello, la comunidad internacional presentó el Convenio de Budapest, también conocido como Convenio sobre la Ciberdelincuencia. El referido convenio fue adoptado en la Sesión N° 109 del Comité de Ministros de Consejo de Europa, el 8 de noviembre de 2001, teniendo como objetivo

[25] Mata y Martín, R. M. Op.cit. Pg. 40.
[26] Vidaurri Aréchiga, M. (2016). Bases de Criminología y Política Criminal. Oxford University Press México, S.A. Pg. 260
[27] Meneses Ochoa, Jean Paul y Meneses Gonzales, Bonifacio (2024). La Cibercriminalidad Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional. Instituto Iberoamericano de Justicia.

principal la consolidación de una política a fin de brindar protección a la comunidad internacional sobre la cibercriminalidad.

Otro tema que debe tener en consideración la Política Criminal aplicada al tratamiento de la ciberdelincuencia, es la complejidad de estas modernas tecnologías que son usadas para la comisión de estos cibercrímenes.

En tal sentido, como se ha señalado anteriormente, Zúñiga Rodríguez señala que la política criminal debe elaborarse en base a estudios científicos para entender las aristas de la problemática social[28].

Asimismo, sobre el uso de la ciencia en la Política Criminal, Martínez Espasa concluyó lo siguiente:

> *Para el correcto establecimiento de programas de prevención y reducción de la delincuencia, los responsables en la materia deben escuchar los criterios científicos existentes para decidir para decidir la mejor opción sobre la aplicación de las políticas públicas de seguridad ciudadana. Pero además, debe consensuarse un marco de trabajo común en el que los políticos, técnicos, profesionales, estudiosos, etc. Puedan intercambiar y comparar información y resultados[29].*

Conforme a lo expuesto, podemos colegir que el uso de la ciencia y tecnología deben ser herramientas primordiales para el diseño de un Política Criminal dirigida a la cibercriminalidad.

De este modo, existe un caso expuesto en un noticiero peruano donde puede verse un caso donde se utilizan conocimientos tecnológicos para denunciar ciberataques. Es así que en este reportaje se registró un caso de dos consultores en ciberseguridad que se infiltraron en una red de hackers que tenían como finalidad de vulnerar la web del bono universal, el cual estaba destinado para ayudar económicamente a las personas afectadas por la pandemia originada por el COVID-19[30].

En ese sentido este caso puede identificarse a lo que se conoce como "hackers de sobre blanco", los cuales dirigen sus acciones a combatir a los hackers con fines ilícitos. En el caso en mención, se puede ver a hackers, utilizando sus conocimientos en ciberseguridad para denunciar a otros hackers ante las autoridades peruanas.

Conforme a lo expuesto, en general las políticas públicas dirigidas para el tratamiento de la cibercriminalidad, si son diseñadas base a estudios de ciencia y tecnología, pueden obtener resultados eficaces en la prevención y procesamiento de los ciberataques.

---

[28] Zúñiga Rodríguez, L. Op.cit. Pp. 47-48.
[29] Martínez Espasa, J. Op.cit. Pg. 131.
[30] Al Estilo Juliana. Radio Mix Purhuaracra Tarma (29 de mayo de 2020). Hackean Web Del Bono Universal Pará Robar Casi Un Millón De Soles. Youtube. https://www.youtube.com/watch?v=Syq-EPEwMz4

De este modo, no resulta absurdo señalar que, en la lucha contra los cibercrímenes, se deberá combatir tecnología con tecnología.

En tal sentido, los órganos jurisdiccionales especializados en cibercrimen como Política Criminal contra la cibercriminalidad, deberá estar diseñada en atención a estudios de ciencia y tecnología, por cuanto estos órganos estarán dirigidos al tratamiento de delitos con particularidades que requieren una atención especializada en tecnología.

Con relación ello nos resulta obvio señalar que no será lo mismo para un magistrado que procese o juzgue un caso de hurto agravado a que procese casos de fraudes informáticos o delitos en el ciberespacio mediante el uso de la inteligencia artificial. De este modo, es evidente que se requieren órganos jurisdiccionales con una especialización en ciberdelitos.

4. SOBRE LA NECESIDAD DE LA IMPLEMENTACIÓN DE LOS ÓRGANOS JURISDICCIONALES ESPECIALIZADOS EN CIBERCRIMINALIDAD EN EL PODER JUDICIAL

Conforme a los datos expuestos provenientes de la Policía Nacional del Perú, Ministerio Público, Poder Judicial, Ministerio de Justicia y Derechos Humanos y Defensoría del Pueblo, podemos observar que los índices de la ciberdelincuencia vienen aumentando año tras año. Esto generaría muchos problemas respecto a la afectación de la seguridad ciudadana, así como la sobrecarga procesal del Sistema Penal.

Por otro lado, realizando una comparación frente a los datos expuestos, en atención a las estadísticas de la Oficina de Control de la Productividad Fiscal (OCPF) de la Base de datos del Sistema de Gestión Fiscal (SGF) y el Sistema de Información de Apoyo al Trabajo Fiscal (SIATF) del Ministerio Público, podemos observar que existe una gran cantidad de delitos informáticos archivados por diferentes motivos. Lo referido es preocupante, por cuanto se estaría generando lo que se conoce como el paraíso de la impunidad.

En atención ello, nos lleva a realizar la siguiente pregunta ¿Qué deben hacer los organismos que componen el Sistema Penal peruano frente a los índices de cibercriminalidad y los índices de impunidad?

Respecto al Diagnóstico Situacional Multisectorial sobre la Ciberdelincuencia en el Perú publicado por el Ministerio de Justicia y Derechos Humanos, podemos observar que las medidas implementadas en el Perú no han sido suficientes para la lucha contra la cibercriminalidad.

En la actualidad no existe una Ley en Ciberseguridad en el Perú que pueda sentar las bases en materia de ciberseguridad. Tampoco se ha implementado una política o Plan gubernamental materia de ciberseguridad o contra la ciberdelincuencia. Esto es grave por cuanto en otros países de la región, como Argentina, Chile, Colombia o Ecuador, cuentan con estas medidas implementadas a fin brindar seguridad de las personas en el ciberespacio.

De igual forma, por parte de las instituciones que componen el Sistema Penal, podemos señalar que no existen protocolos institucionales o interinstitucionales para el tratamiento de la ciberdelincuencia. Asimismo, tampoco existe una estrategia de coordinación entre el Poder Judicial, Ministerio Público y la Policía Nacional del Perú.

Solamente la Policía Nacional del Perú y el Ministerio Público, han implementado organismos especializados para el tratamiento de la cibercriminalidad. Sin embargo, a pesar de los esfuerzos de las instituciones mencionadas, el Poder Judicial no ha implementado estrategias u órganos especializados frente a la cibercriminalidad.

Aunado a ello, en el Informe de Análisis N° 04 – Ciberdelincuencia en el Perú: Pautas para una Investigación Fiscal Especializada, con el objetivo de conocer la experiencia, percepción y opinión de los fiscales en la investigación de los delitos informáticos, se diseñó un cuestionario de 21 preguntas, el mismo que fue aplicado por vía correo electrónico y la plataforma Google Forms a 8 Fiscales de las Fiscalías Provinciales Penales de mayor incidencia de denuncias por delitos informáticos en el periodo de octubre 2013 a julio 2020[31].

En la referida muestra realizada a los 8 Fiscales de las fiscalías provinciales, indicaron que tuvieron dificultades en la investigación y enjuiciamiento en la ciberdelincuencia. Respecto a las diligencias preliminares, se indica que tuvieron dificultades relacionadas al identificar al autor y poca información, los jueces se niegan el levantamiento del secreto a las telecomunicaciones (art. 230 del NCPP), así como necesidad de equipos de alta tecnología para identificar autores.

También se indicó como dificultades los insuficientes o deficientes órganos de apoyo. Se precisa que la referida dificultad consistió en la falta de capacitación de los policías en uso de técnicas de investigación especial y falta de peritos en la materia.

Respecto a la etapa de formalización y continuación de la investigación preparatoria, se indicó que tuvieron problemas por cuanto la falta de capacidades tecnológicas de la Policía Nacional del Perú, falta de peritos y en la cooperación con otras Fiscalías para investigar imputados que se encuentran fuera del Distrito Fiscal.

En la etapa de juicio oral, los fiscales indicaron que tuvieron problemas respecto a la poca asistencia de los peritos al juicio oral y a la ubicación de los órganos de prueba, agraviado y efectivos policiales para la participación en el proceso.

Conforme a lo recogido del Informe de Análisis N° 04 – Ciberdelincuencia en el Perú: Pautas para una Investigación Fiscal Especializada, entendemos que la referida encuesta fue realizada a fiscales de 8 fiscalías, sin embargo, esto nos

[31] Ministerio Público – Fiscalía de la Nación. Op.cit. Pg. 35-42

es útil a fin de estudiar la problemática en la investigación y procesamiento de la ciberdelincuencia.

En atención a los datos expuestos por parte de las entidades públicas encargadas de la persecución penal y procesamiento de los delitos informáticos, resulta evidente la necesidad de implementar acciones preventivas para la persecución y sanción de los ciberdelitos.

Aunado a ello, en el mes de mayo de 2023, la Defensoría del Pueblo publica el Informe Defensorial N° 001-2023-DP/ADHPD (La Ciberdelincuencia en el Perú: Estrategias y Retos del Estado) por medio del cual presenta un diagnóstico de la situación de la cibercriminalidad en el Perú, como se manifiesta y la forma de como el Estado debe atenderla, protegiendo a la ciudadanía.

En atención a la facultad constitucional que posee la Defensoría del Pueblo, en referencia a la promoción y defensa de los derechos constitucionales, así como su competencia en la supervisión de los diferentes órganos que componen el sistema de justicia, elabora el Informe Defensorial N° 001-2023-DP/ADHPD.

Al respecto, debemos reconocer la labor que viene realizado la Defensoría del Pueblo, sin embargo, criticamos que su informen en cuestión, posee varios tópicos que ya fueron desarrollados en informes elaborados por el Ministerio Público y el Ministerio de Justicia y Derechos Humanos.

Sin embargo, el informe de la Defensoría del Pueblo se diferencia en las conclusiones y recomendaciones, las cuales podemos resaltar las siguientes:

> ***Conclusiones***
> *(...) 5.19. Entre los años 2015 y 2019, el Poder Judicial condenó a 397 personas por la comisión de ciberdelitos previstos en la Ley de Delitos Informáticos, lo que representa apenas el 2% de las denuncias registradas por el Ministerio Público en dicho periodo. Al respecto es relevante advertir que en la actualidad es la única institución del sistema de justicia que aún no ha implementado órganos especializados en ciberdelincuencia, sin embargo, no es posible afirmar de la supervisión realizada si ello se debe a que no se considera necesario debido a que no existe una excesiva demanda de casos o por otros factores.*
>
> ***Recomendaciones***
> *(...)* ***Al Poder Judicial***
> *6.24. Evaluar la implementación de un subsistema de justicia especializado en ciberdelincuencia, con personal debidamente capacitado, para conocer casos sobre delitos informáticos y otros que se realizan con el uso de las tecnologías de la información y las comunicaciones.*[32] (el subrayado es nuestro)

[32] Defensoría del Pueblo. (2023) Informe Defensorial N° 001-2023-DP/ADHPD – La Ciberdelincuencia en el Perú: Estrategias y retos del Estado. Pp. 65-69. Recuperado el 21 de

Conforme a lo expuesto, se resalta que la Defensoría del Pueblo identifica la problemática actual en el Poder Judicial respecto al tratamiento de la cibercriminalidad, por cuanto solo ha condenado a 397 personas, advirtiendo que es el único que no tiene órganos especializados en la lucha contra el cibercrimen, a diferencia de la Policía Nacional del Perú y el Ministerio Público.

De igual forma, es importante la recomendación de la implementación de órganos jurisdiccionales especializados para el procesamiento de la cibercriminalidad, por cuanto el Poder Judicial debe estar alineado con la Policía Nacional del Perú y el Ministerio Público quienes han entendido que este fenómeno criminal requiere un tratamiento especializado en atención a sus características y sus sofisticaciones tecnológicas.

Es así que la implementación de los órganos jurisdiccionales especializados en cibercriminalidad es una necesidad real, por cuanto debido a los avances tecnológicos han ocasionado la aparición de una nueva criminalidad que utiliza la tecnología para realizar crímenes en un nuevo ámbito como lo es el ciberespacio.

En conclusión, la presente propuesta de ley que ley que declara de interés nacional y necesidad pública la implementación de los órganos jurisdiccionales especializados en cibercriminalidad es una iniciativa necesaria y urgente. La creciente sofisticación de los delitos informáticos exige una respuesta igualmente sofisticada por parte del sistema judicial. Al contar con jueces y fiscales especializados, se podrá garantizar una mayor eficiencia en la investigación y el enjuiciamiento de estos delitos, lo que a su vez contribuirá a disuadir a los cibercriminales y a proteger a la sociedad en su conjunto.

Es fundamental que las instituciones públicas reconozcan la importancia de esta propuesta y trabajen de manera conjunta para su implementación efectiva. En tal sentido, resulta necesario contar con un sistema de justicia preparado ante esta nueva criminalidad, lo que significa contar con no solo con defensores públicos, policías y fiscales especializados en cibercriminalidad, sino también con órganos jurisdiccionales, por cuanto este tipo de criminalidad requiere una atención especializada en nuevas tecnologías y ciberataques en el ciberespacio. La ciberseguridad es un desafío global que requiere soluciones globales, y la implementación de órganos jurisdiccionales especializados es un paso fundamental en esta dirección.

---

noviembre de 2023 de: https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

II. MARCO NORMATIVO

- Constitución Política del Perú
- Convenio Sobre la Ciberdelincuencia de Budapest
- Decreto Legislativo N°957, del 29 de Julio de 2004, que promulga el Código Procesal Penal (CPP).
- Decreto Legislativo N°635, Código Penal.
- Decreto Legislativo N° 1407, que fortalece la Defensa Publica.
- Decreto Legislativo Nº 052, Ley Orgánica del Ministerio Público
- Decreto Legislativo N°1267, Ley de la Policía Nacional del Perú
- Ley 29158, Ley Orgánica del Poder Ejecutivo
- Ley 29360, Ley del Servicio de Defensa Publica.
- Ley N° 27309, Ley que incorpora los Delitos Informáticos al Código Penal
- Ley N° 30096, Ley de Delitos Informáticos
- Ley 30999, Ley de Ciberdefensa.
- Ley 30618, Ley que modifica el Decreto Legislativo 1141, Decreto Legislativo de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional (SINA) y de la Dirección Nacional de Inteligencia (DINI), a fin de regular la Seguridad Digital.
- Decreto Supremo 012-2017-DE, Decreto Supremo que aprueba la Política de Seguridad y Defensa Nacional.
- Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Supremo N° 029-2021 PCM, que aprueba si Reglamento de la Ley de Gobierno Digital
- Decreto Supremo 050-2018-PCM, Decreto Supremo que establece la definición de Seguridad Digital de ámbito nacional.
- Decreto de Urgencia 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Decreto Supremo N° 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia N" 006-2020. Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital
- Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Constitución Política del Perú

III. ANTECEDENTES DE LA PROPUESTA LEGISLATIVA

De una revisión general de proyectos de ley en la Plataforma del Congreso de la República NO se identificó alguna iniciativa relacionada con nuestra propuesta normativa.

IV. EFECTO DE VIGENCIA DE LA NORMA SOBRE LA LEGISLACIÓN NACIONAL

La presente iniciativa legislativa no colisiona con ninguna norma vigente. La propuesta es de carácter **declarativa**, no contraviene ninguna disposición legal del ordenamiento jurídico peruano y versa exclusivamente sobre la declaración de interés nacional y necesidad pública la implementación de los órganos jurisdiccionales especializados en cibercriminalidad.

V. ANÁLISIS COSTO-BENEFICIO

La presente propuesta de Ley propone declarar de interés nacional y necesidad pública la implementación de los órganos jurisdiccionales especializados en cibercriminalidad, esta propuesta no implicará asumir costos adicionales a los ya existentes por cuanto solamente se deberán realizar coordinaciones entre el Ministerio de Economía y Finanzas y el Poder Judicial, a fin de lograr esta importante implementación. La cibercriminalidad representa una amenaza constante para la seguridad nacional, la economía y los derechos fundamentales de las personas.

La implementación de los órganos jurisdiccionales especializados en cibercriminalidad representa un paso crucial en la lucha contra la creciente ola de delitos informáticos. En un mundo cada vez más digitalizado, donde las transacciones comerciales, la comunicación y la interacción social se llevan a cabo principalmente a través de medios electrónicos, la cibercriminalidad ha evolucionado a una escala sin precedentes, exigiendo respuestas ágiles y efectivas por parte de los sistemas judiciales.

Por ello se necesita contar con un marco jurídico especializado y personal altamente capacitado para enfrentar la complejidad y la dinámica propia de los delitos cibernéticos. Los delincuentes informáticos operan en un entorno transfronterizo, utilizando herramientas tecnológicas sofisticadas y explotando las vulnerabilidades de los sistemas informáticos. Ante esta realidad, los sistemas judiciales tradicionales, diseñados para abordar delitos físicos, se encuentran desbordados y con dificultades para investigar y sancionar de manera adecuada estos nuevos tipos de crímenes.

La implementación de órganos jurisdiccionales especializados en cibercriminalidad permitiría contar con jueces y fiscales con conocimientos técnicos en informática y derecho penal, capaces de comprender la naturaleza de los delitos informáticos, analizar la evidencia digital y aplicar las normas legales pertinentes. Además, estos órganos podrían desarrollar protocolos y procedimientos específicos para la investigación y el enjuiciamiento de estos delitos, garantizando así una mayor eficiencia y eficacia en la persecución de los cibercriminales.

VI. RELACIÓN CON LAS POLÍTICAS DE ESTADO DEL ACUERDO NACIONAL

El presente proyecto de Ley guarda armonía con el Acuerdo Nacional respecto a los siguientes puntos:

ACUERDO NACIONAL	
I. DEMOCRACIA Y ESTADO DE DERECHO	7. ERRADICACIÓN DE LA VIOLENCIA Y FORTALECIMIENTO DEL CIVISMO Y DE LA SEGURIDAD CIUDADANA
III. COMPETITIVIDAD EN EL PAÍS	20. DESARROLLO DE LA CIENCIA Y LA TECNOLOGÍA
IV. ESTADO EFICIENTE, TRANSPARENTE Y DESCENTRALIZADO	24. AFIRMACIÓN DE UN ESTADO EFICIENTE Y TRANSPARENTE
	28. PLENA VIGENCIA DE LA CONSTITUCIÓN Y DE LOS DERECHOS HUMANOS Y ACCESO A LA JUSTICIA E INDEPENDENCIA JUDICIAL

VII. RELACIÓN CON LA AGENDA LEGISLATIVA 2023-2024

Con relación a la Agenda Legislativa para el periodo 2023-2024 aprobada por Resolución Legislativa del Congreso N° 002-2023-2024-CR, publicada el 17 de octubre de 2023 y vigente a la fecha, se cumple con los siguientes temas:

- Tema 18. MEDIDAS EN FAVOR DE LA SEGURIDAD CIUDADANA Y EL CIVISMO
- Tema 89. SOBRE CIENCIA, INNOVACIÓN Y TECNOLOGÍA
- Tema 100. MODERNIZACIÓN Y EFICIENCIA DE LA GESTIÓN DEL ESTADO Y LA ADMINISTRACIÓN PÚBLICA
- Tema 105. MODERNIZACIÓN Y ACCESO EN EL SISTEMA DE JUSTICIA