6.4 **Adultos mayores y tercera edad**

Al inicio de este análisis se ha incluido a las personas que integran este colectivo como especialmente vulnerables frente a las actividades ilícitas que se cometen en el ciberespacio. Es esta una apreciación cada vez más evidente, al constatar las consecuencias que está generando en nuestros mayores la evolución tecnológica y otra serie de factores concurrentes. Así, es obvio que la progresiva digitalización de todo tipo de actividades, entre ellas las de carácter económico y/o financiero o las relacionadas con la prestación de cualquier clase de servicios –incluidos los de carácter esencial como la electricidad o el suministro de agua o gas–, ha determinado que la realización de muchos de los trámites relacionados con ello actualmente se hayan de llevar a efecto en forma telemática, circunstancia a la que tampoco es ajena la situación generada con ocasión de la pandemia y el obligado aislamiento social de la población por periodos prolongados de tiempo. En consecuencia, las personas mayores se han visto obligadas a asumir esta nueva dinámica de forma precipitada y sin que las circunstancias hayan hecho posible prestarles el apoyo necesario para facilitarles la transición a una inédita forma de relación incuestionablemente compleja y que exige, necesariamente, ciertos conocimientos básicos para poder desenvolverse con normalidad y de forma segura.

Los efectos derivados de esta situación se han ido percibiendo con crudeza, no solo durante el periodo de confinamiento sino también en los meses posteriores. Son muchos los casos de personas mayores que han sido captadas por desaprensivos que, aprovechándose de su desamparo, su situación de miedo y preocupación y su inexperiencia en el uso de las TIC, les han engañado utilizando diversas técnicas –haciéndose pasar por empleados de su entidad bancaria, de la compañía aseguradora, o de la empresa eléctrica prestadora del servicio, etc.– para, de esta forma, lograr acceder a sus claves y contraseñas bancarias o a la información alojada en sus dispositivos para apoderarse de sus ahorros. Como también han sido frecuentes los supuestos en que los delincuentes se han dirigido a través de la red a estas personas con ofertas fraudulentas de bienes y servicios, en ocasiones relacionados con una supuesta protección de su salud, consiguiendo de esa manera la entrega de cantidades de dinero sin contraprestación alguna. Además, en ocasiones, los criminales han aprovechado estos contactos para tomar conocimiento de la documentación y datos personales de sus víctimas que posteriormente han utilizado, usurpando dicha identidad, en actuaciones diversas, tales como adquisición de productos, contratación de servicios, apertura de líneas de crédito e,

incluso, planificación y ejecución, con esa identidad supuesta, de fraudes a terceros, generando así nuevos y más graves perjuicios económicos y morales para los afectados.

Ciertamente, esta situación no afecta exclusivamente a las personas mayores de edad sino a todos los ciudadanos y ciudadanas en mayor o menor medida, pero es precisamente este colectivo el que se encuentra, por las circunstancias antedichas, en situación de especial vulnerabilidad.

Corresponde al Ministerio Fiscal, en su función constitucional de defensor de los derechos de todos los ciudadanos, actuar con eficacia frente a estas conductas y proteger los intereses de quienes han sido víctimas de estos comportamientos. Desde el área de especialización en criminalidad informática y, teniendo en cuenta el ámbito de actuación que nos compete, los esfuerzos se orientan en varias direcciones que resumimos a continuación:

– Impulsar la coordinación en la investigación de estas conductas delictivas.

En muchos de estos supuestos los/as delincuentes planifican sus actuaciones ilícitas de forma tal que afecten en cuantías no excesivamente elevadas a una pluralidad de perjudicados/as diseminados por distintos territorios. Como consecuencia de ello, el análisis independiente de las distintas denuncias presentadas por los múltiples afectados/as, la escasa cuantía del perjuicio causado individualmente –que, por razones de proporcionalidad, dificulta el uso herramientas de investigación limitativas de derechos– y el empleo por los criminales de técnicas diversas de anonimización u ocultación de identidad, abocan en gran número de ocasiones al archivo del procedimiento judicial o de las diligencias policiales incoadas para su esclarecimiento.

Para evitar este indeseable efecto, se recurre en la Unidad a los *expedientes de coordinación* que, con base en la Instrucción 2/2011 y la colaboración imprescindible de los/as delegados/as y las Oficinas de Enlace con los Cuerpos Policiales, tienen por objeto acumular y analizar conjuntamente toda la información relativa a una misma acción criminal con efectos en distintos territorios, a fin de orientar centralizadamente la investigación; coordinar sus resultados y, si fuera procedente, promover la acumulación de los diversos procedimientos ante el órgano judicial que sea competente.

De esta forma se intenta paliar, en la medida de lo posible y pese a los escasos recursos de los que se dispone, las perversas consecuencias de una planificación criminal que, mediante la dispersión territorial de los efectos del delito, busca obstaculizar la actuación policial y

judicial y, a la postre, hacer ilusoria la reparación de los perjuicios causados a los/las afectados/as. No obstante, no se desconoce que esta coordinación que se desarrolla desde la Unidad especializada, casi de forma artesanal, es claramente insuficiente para solventar las dificultades mencionadas. Es por ello que se promueve desde hace tiempo la solución adoptada en el marco del Plan Estratégico Nacional contra la Ciberdelincuencia de articular una base de datos nacional en la que se recopile toda la información registrada con ocasión de las denuncias y atestados por ciberdelitos, particularmente sobre defraudaciones *online*, de los distintos cuerpos policiales nacionales o autonómicos, de forma tal que sea posible entrecruzar los datos obtenidos y relacionar entre sí las múltiples actividades ilícitas que se registran anualmente, ello con el objetivo de facilitar la investigación de dichas conductas y, en consecuencia la reparación de quienes hayan resultado perjudicados.

– Ofrecer soluciones efectivas ante el progresivo incremento de supuestos de suplantación de identidad *online* con fines defraudatorios.

Es esta otra cuestión vinculada a la anterior que preocupa seriamente tanto al MF como a los cuerpos policiales ya que, como se ha indicado, cada vez es más habitual que los/as delincuentes aprovechen documentación personal de terceros, obtenida irregularmente, para usurpar su identidad en cualquier clase de operaciones económicas en beneficio propio y también para contactar *online* con terceros con fines espurios y/o abrir cuentas bancarias específicamente destinadas a canalizar la entrega de las cantidades fraudulentamente obtenidas, o para ocultar ganancias ilícitas y facilitar su aprovechamiento definitivo. Como consecuencia de ello, son frecuentes los supuestos de incoación de procedimientos judiciales dirigidos contra personas que no solamente carecen de responsabilidad alguna en el hecho delictivo que se les imputa, sino que incluso han sido perjudicadas directamente por esa misma actividad criminal en fases anteriores de la ejecución delictiva.

Esta anomalía ha determinado que la red de especialistas en Criminalidad Informática trabaje para paliar en la medida de lo posible estas situaciones. A dicho fin, en la Unidad especializada se han incoado, por el momento, un total de 109 de expedientes relativos a supuestos de esta naturaleza –56 de los cuales corresponden a 2021 y 33 al tiempo transcurrido de la presente anualidad– en los que, con la colaboración de los/as delegados/as y de nuestras Oficinas de Enlace con los cuerpos policiales, se recopila toda la información disponible acerca de atestados/procedimientos judiciales dirigidos contra

la persona cuya identidad ha sido supuestamente usurpada. Tal información, junto con la documentación complementaria que se estime necesaria, se traslada a los/as delegados/as en los territorios en que se tramitan las correspondientes acciones judiciales para alertarles sobre la concurrencia de la indicada circunstancia a fin de que puedan valorarla adecuadamente en cada uno de dichos procedimientos. Asimismo, desde la Unidad se promueve una atención más cuidadosa por parte de todos los integrantes de la Institución que permita detectar a tiempo estas situaciones y corregir los errores en la identificación de los presuntos responsables criminales en los procesos en curso, evitando de esta forma las consecuencias que de ello se derivan para los afectados/as.

Ciertamente el esfuerzo que está volcando la Institución para solventar los problemas que se han ido exponiendo en este apartado resulta insuficiente, por sí mismo, para garantizar plenamente los derechos e intereses de las víctimas de los ciberdelitos, cualesquiera que sean sus circunstancias, y repararles en los perjuicios sufridos. A esos efectos, es necesaria una actuación coordinada con otros organismos e instituciones con responsabilidad en cada una de las materias. Sin perjuicio de ello la dinámica adoptada deja constancia de nuestra voluntad de dar cumplimiento a las funciones que corresponden al Ministerio Fiscal de protección de los derechos e intereses de quienes se han visto afectados por actividades criminales de una u otra naturaleza.