

**A LA MESA DEL CONGRESO DE LOS DIPUTADOS**

D. Vicente Ten Oliver, Diputado del Grupo Parlamentario de Ciudadanos, al amparo de lo dispuesto en el artículo 185 y siguientes, del vigente Reglamento de la Cámara, presenta la siguiente pregunta para la que se solicita respuesta por escrito **sobre el uso de nuevas tecnologías en la financiación de actividades ilícitas.**

Congreso de los Diputados, 15 de diciembre de 2017

**EXPOSICIÓN DE MOTIVOS**

Aunque tecnologías como la “deep web” o “blockchain” nacieron buscando proteger la privacidad de los usuarios encriptando la información, esta opacidad puede por motivos obvios resultar muy conveniente para el desarrollo de actividades ilegales.

La tecnología conocida como “blockchain”, cadena de bloques, permite realizar transacciones seguras de forma descentralizada, es decir sin contar con un intermediario oficial que de fe y seguridad a dicha transacción. Esta tecnología está detrás de las criptomonedas, monedas digitales que cumplen con las funciones clásicas del dinero de: unidad de cuenta, depósito de valor y forma de pago.

El uso de las monedas virtuales se han extendido hasta llegar a más de 900 monedas digitales, aunque la más popular y usada en bitcoin. Actualmente se estima que estas redes mueven más de 700 millones de dólares.

El pasado mes de junio de 2017, el Centro Europeo de Ciberdelincuencia (EC3) de Europol organizó la 4ª Conferencia de Monedas Virtuales. El objetivo principal de esta conferencia era fortalecer la lucha contra el abuso de las monedas virtuales para las transacciones delictivas y el lavado de dinero.

Un caso reciente y muy relevante del uso de las criptomonedas para burlar la ley se encuentra en Cataluña. Noticias recientes aseguran que la Guardia Civil encontró anotaciones del jefe de Riesgos de Cescicat (Centro de Seguridad de la Información de Cataluña) para adquirir la criptomoneda digital Ethereum y Bitcoins para ocultar los pagos por los 140 dominios web con los que se organizó el referéndum del 1 de octubre, declarado ilegal por el Tribunal Constitucional.

Aunque la recientemente publicada Estrategia de Seguridad Nacional 2017, hace varias referencias a la lucha contra la financiación del terrorismo y dedica una atención particular a la ciberseguridad, en ningún momento estas dos cuestiones se entrecruzan. Además esta estrategia en ningún caso menciona las criptomonedas o a la internet profunda cómo focos de riesgo.

Parece razonable pensar que con un creciente porcentaje de la actividad comercial trasladándose a internet también habrá un porcentaje mayor de actividades ilícitas que se realizan en la red. Las empresas invierten cada vez más recursos en ciberseguridad, creando un demanda para una nueva industria.

El Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (Onsi) publicó en 2016 el único estudio oficial hasta la fecha sobre el “subsector y el mercado de la ciberseguridad”.

En cuanto al análisis de la oferta, en España en 2014 había 533 empresas en el subsector de la ciberseguridad, dando empleo a 5.808 personas, con una facturación que se sitúa ese mismo año en 598 millones de euros (el 0,06% del PIB) y una inversión que asciende a 79 millones de euros. Las empresas dedicadas exclusivamente al subsector de la ciberseguridad (un 14,8 % del total de las 533 empresas), han contribuido a más del 50 % de la facturación total del subsector.

En relación a la demanda, el estudio determina que los productos más demandados en España son los cortafuegos (41,9 millones de euros) y la externalización de los servicios de seguridad (55,6 millones de euros). En la previsión de crecimiento de la demanda a 3 y 5 años en productos de ciberseguridad por las empresas y los particulares, destaca el incremento en la demanda de productos por las empresas se producirá en las auditorías de red (45,3 %) y en la externalización de servicios de ciberseguridad (45,1 %), de 2014 a 2019. El estudio prevé que la demanda en España por particulares se aumente un 11,1 % para el mismo periodo.

Por último, aunque el presupuesto en PGE del Instituto Nacional de Ciberseguridad (INCIBE), antes Instituto Nacional de Tecnologías de la Comunicación (INTECO), se ha más que duplicado entre 2007 y 2017 pasando de 10 millones a 23,2 millones de euros, esto es sólo parte insignificante del presupuesto total de las políticas de defensa y seguridad ciudadana y penitenciaria cercano a los 16.000 millones de euros.

Por todo lo anterior, se formulan las siguientes preguntas:

- 1.- ¿Qué papel estima el gobierno que tienen las criptomonedas en la financiación de actividades ilícitas como el tráfico de armas, el terrorismo, el narcotráfico o la trata de seres humanos?
- 2.- ¿Qué recursos está destinando el gobierno a labores de policía en transacciones con criptomonedas?
- 3.- ¿Qué medidas está desarrollando el gobierno para impulsar una industria nacional de ciberseguridad?
- 4.- ¿Tiene el gobierno alguna estimación del coste que supone a España la ciberdelincuencia?



Vicente Ten Oliver  
Diputado del Grupo Parlamentario de Ciudadanos