Dictamen del Comité Económico y Social Europeo sobre la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión

[COM(2013) 48 final — 2013/0027 (COD)]

(2013/C 271/25)

Ponente: **Sr. McDONOGH**

El 21 de febrero y el 15 de abril de 2013, de conformidad con el artículo 114 del Tratado de Funcionamiento de la Unión Europea, el Consejo y el Parlamento Europeo respectivamente decidieron consultar al Comité Económico y Social Europeo sobre la

Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión

COM(2013) 48 final – 2013/0027 (COD).

La Sección Especializada de Transportes, Energía, Infraestructuras y Sociedad de la Información, encargada de preparar los trabajos en este asunto, aprobó su dictamen el 30 de abril de 2013.

En su 490º pleno de los días 22 y 23 de mayo de 2013 (sesión del 22 de mayo de 2013), el Comité Económico y Social Europeo aprobó por 163 votos a favor, 1 en contra y 5 abstenciones el presente dictamen.

1. **Conclusiones y recomendaciones**

1.1 El Comité toma nota de la propuesta de Directiva, que debería considerarse en el contexto más amplio de la reciente publicación de la Estrategia de ciberseguridad ([1]), y que esboza una visión integral de la seguridad de las redes y de la información (SRI) al objeto de garantizar que la economía digital puede prosperar de manera segura, sin dejar de promover cada vez más los valores europeos de la libertad y la democracia.

1.2 El CESE acoge con satisfacción esta propuesta de Directiva para asegurar un elevado nivel común de SRI en la Unión. La armonización y la gestión de la SRI a escala europea revisten suma importancia para la realización del mercado único digital y el buen funcionamiento del mercado interior en su conjunto. El Comité comparte las inquietudes de la Comisión por el enorme daño que un fallo de SRI podría ocasionar a la economía y el bienestar de los ciudadanos. Sin embargo, la propuesta de Directiva no cumple las expectativas del Comité por lo que respecta a una acción legislativa enérgica en una cuestión crítica como esta.

1.3 El Comité muestra su enorme decepción por la falta de avances en la aplicación de una SRI eficaz a nivel nacional en numerosos Estados miembros. El CESE lamenta el aumento de los riesgos que un fallo de estas características genera para los ciudadanos, así como la repercusión negativa que conlleva para la realización del mercado único digital. Todos los Estados miembros han de tomar medidas sin mayor dilación respecto de sus obligaciones pendientes en materia de SRI.

1.4 Esta falta de avances está abriendo otra grieta digital entre un grupo de élite dotado de una RSI muy avanzada y otros Estados miembros que han realizado menos progresos. Esta brecha está perjudicando a la confianza y la colaboración en SRI a escala de la UE y, si no se aborda de manera urgente, es probable que ocasione deficiencias del mercado único asociadas con las diferencias de capacidad entre los Estados miembros.

1.5 Como ya se ha señalado en dictámenes precedentes ([2]), el CESE considera que las medidas indicativas y voluntarias no funcionan y que los Estados miembros deben contar con obligaciones reglamentarias fuertes para garantizar la armonización, la gobernanza y el cumplimiento de la SRI en Europa. Desgraciadamente, el CESE no cree que esta propuesta de Directiva vaya a proporcionar la legislación clara y decisiva que se necesita. Para facilitar un elevado nivel común de RSI, el Comité opina que un reglamento que impusiera a los Estados miembros obligaciones bien definidas sería más eficaz que una directiva.

1.6 A pesar de la pretensión de la Comisión Europea de adoptar delegados para garantizar algunas condiciones uniformes de ejecución de partes de la Directiva, el Comité percibe una escasez de normas, de definiciones claras y de obligaciones categóricas en el acto propuesto, lo que ofrece demasiada flexibilidad a los Estados miembros sobre cómo deben interpretar e incorporar los elementos críticos. El Comité echa de menos en el acto definiciones mucho más explícitas de las normas, requisitos y procedimientos que deberán respetar los Estados miembros, los poderes públicos, los operadores del mercado y los principales habilitadores de Internet.

([1]) «Un ciberespacio abierto, protegido y seguro», JOIN (2013) 1.

([2]) «Protección de infraestructuras de información críticas»: DO C 255 de, 22.9.2010, p. 98 y «Directiva relativa a los ataques contra los sistemas de información» DO C 218 de, 23.7.2011, p. 130.

1.7 A fin de ofrecer una formulación y ejecución sólidas en la UE de las políticas en materia de SRI, el Comité aboga por la creación de una autoridad a nivel de la UE para la seguridad de las redes y de la información, similar a la autoridad central de la industria aeronáutica (EASA) ([3]). Este organismo establecería normas y realizaría un seguimiento de la aplicación de todos los elementos de la SRI en el conjunto de la Unión, desde la certificación de terminales seguros y su utilización, hasta la seguridad de la red y la seguridad de los datos.

1.8 El CESE es muy consciente de que la adopción en Europa de la computación en nube ([4]) comporta mayores riesgos en el ámbito de la ciberseguridad y la protección de los datos. El Comité desearía que la propuesta legislativa incluyera explícitamente más requisitos y obligaciones especiales de seguridad en relación con la prestación y uso de los servicios en nube.

1.9 Para lograr que se rindan cuentas debidamente en cuestiones de SRI, el acto debe dejar claro que las entidades con obligaciones según la propuesta de Directiva tendrán derecho a hacer responsables a sus suministradores de programas informáticos y de equipos físicos de cualquier deficiencia en sus productos o servicios que coadyuvara directamente a un incidente de SRI.

1.10 El CESE pide a los Estados miembros que presten especial atención para reforzar los conocimientos en SRI y las capacidades en materia de ciberseguridad de las pequeñas y medianas empresas (PYME). El Comité también llama la atención de la Comisión sobre el éxito de las competiciones de *hackers* en los EE.UU. ([5]) y en algunos Estados miembros ([6]), a la hora de sensibilizar sobre la ciberseguridad e instruir a la próxima generación de profesionales de la SRI.

1.11 Dada la importancia que reviste la observancia en el conjunto de los Estados miembros de la seguridad de las redes y de la información de toda la UE, el CESE pide a la Comisión que considere qué financiación del Marco Financiero Plurianual (MFP) podría asignarse a tales efectos para asistir a los Estados miembros que necesitaran ayuda económica.

1.12 El gasto en investigación, desarrollo e innovación (I+D+i) en favor de las tecnologías de SRI debe ocupar un lugar prioritario en el Programa Marco de Investigación e Innovación de la UE «Horizonte 2020» para que Europa no se quede rezagada en un escenario en tan rápida mutación como es el de las amenazas cibernéticas.

1.13 Para ayudar a aportar claridad sobre cuáles son las entidades que deberán asumir responsabilidades legales de conformidad con el acto propuesto, el CESE considera deseable la obligatoriedad de que cada Estado miembro publique un directorio en línea en el que figuren todas las entidades que cumplan los requisitos de gestión del riesgo e información que exige la Directiva. La transparencia y la rendición pública de cuentas contribuirán a generar confianza y a que se cumplan las normas.

1.14 El Comité remite a la Comisión a los numerosos dictámenes anteriores del CESE en los que se ha debatido el tema de la seguridad en la red y en la información y que señalaban la necesidad de una sociedad de la información segura y de la protección de las infraestructuras críticas ([7]).

2. **Síntesis de la propuesta de la Comisión**

2.1 La Directiva SRI que se propone se publicó al mismo tiempo que la estrategia de la UE sobre ciberseguridad, que tiene por objeto reforzar la resiliencia de los sistemas de información, reducir la ciberdelincuencia, mejorar la política de ciberseguridad y de ciberdefensa internacional de la UE y desarrollar los recursos industriales y tecnológicos de la ciberseguridad, al mismo tiempo que se promueven los derechos fundamentales y otros valores esenciales de la UE.

2.2 La seguridad de las redes y de la información se ocupa de la protección de Internet y de otras redes, sistemas de información y servicios de apoyo en los que descansa el funcionamiento de nuestra sociedad, y es indispensable para el correcto funcionamiento del mercado único.

2.3 El planteamiento meramente voluntario seguido hasta la fecha por la UE en relación con la SRI no ofrece protección suficiente frente a los riesgos que ella conlleva. Las capacidades de SRI actuales son insuficientes para seguir el paso a un mundo sometido a amenazas en rápida mutación y para garantizar un nivel elevado de protección igual en todos los Estados miembros.

([3]) Agencia Europea de Seguridad Aérea: http://easa.europa.eu/

([4]) «La computación en nube en Europa» DO C 24 de, 28.1.2012, p. 40 y «Liberar el potencial de la computación en nube en Europa» DO C 76 de, 14.3.2013, p. 59.

([5]) http://www.nytimes.com/2013/03/25/technology/united-states-wants-to-attract-hackers-to-public-sector.html?pagewanted=all&_r=0

([6]) http://www.bbc.co.uk/news/technology-17333601

([7]) «Una estrategia para una sociedad de la información segura»: DO C 97 de, 28.4.2007, p. 21.
«Protección de infraestructuras críticas de información»: DO C 255 de, 22.9.2010, p. 98.
« "Nuevo" Reglamento ENISA»: DO C 107 de, 6.4.2011, p. 58.
«Reglamento general de protección de datos»: DO C 229 de, 31.7.2012, p. 90.
«Ataques contra los sistemas de información»: DO C 218 de, 23.7.2011, p. 130.
«Transacciones electrónicas en el mercado interior»: DO C 351 de, 15.11.2012, p. 73.
«Liberar el potencial de la computación en nube en Europa»: DO C 76 de, 14.3.2013, p. 59.

2.4 En la actualidad, los Estados miembros presentan niveles de capacidad y preparación muy distintos, que dan lugar a enfoques fragmentados en la UE en materia de SRI. Al estar redes y sistemas interconectados, los Estados miembros con un nivel insuficiente de protección perjudican a la SRI global de la Unión. Esta situación dificulta asimismo la creación de lazos de confianza entre homólogos, requisito previo para la cooperación y el intercambio de información. Como consecuencia de ello, solamente unos pocos Estados miembros mantienen relaciones de cooperación con elevado nivel de capacidades.

2.5 De conformidad con el artículo 114 del TFUE, el cometido de la Directiva estriba en facilitar la realización y el buen funcionamiento del mercado único digital:

— instaurando un nivel mínimo de SRI en los Estados miembros e incrementando de este modo el nivel global de preparación y respuesta ante incidentes;

— mejorando la cooperación en materia de SRI a escala de la UE para hacer frente a incidentes y amenazas transfronterizos, y

— creando una cultura de gestión de riesgos y mejorando el intercambio de información entre los sectores público y privado.

2.6 La Directiva propuesta establece unos requisitos jurídicos entre los que figuran:

a) los Estados miembros están obligados a adoptar una estrategia de SRI y a designar una autoridad competente para SRI dotada de los recursos económicos y humanos necesarios para impedir, gestionar y responder a riesgos e incidentes de SRI;

b) la creación de un mecanismo de cooperación entre los Estados miembros y la Comisión para compartir alertas tempranas sobre riesgos e incidentes, cooperar y organizar regularmente revisiones por homólogos, y

c) la obligación a determinados tipos de entidad de toda la UE de adoptar prácticas de gestión de riesgos y de notificar a sus autoridades competentes los incidentes de SRI que tengan efectos significativos en sus servicios básicos. Entre las entidades sujetas a estos requisitos figuran los operadores de infraestructuras de información críticas de algunos sectores (servicios financieros, transportes, energía, sanidad), los habilitadores de servicios de la sociedad de la información (especialmente, computación en nube, plataformas de comercio electrónico, pasarelas de pago por Internet, motores de búsqueda, tiendas de aplicaciones y redes sociales) y las administraciones públicas.

2.7 Los Estados miembros deberán transponer la Directiva antes de que transcurran dieciocho meses desde su aprobación por parte del Consejo y del Parlamento Europeo (prevista para 2014).

3. **Observaciones generales**

3.1 El crecimiento de Internet y de la sociedad digital repercute profundamente en la vida cotidiana. Sin embargo, a medida que aumenta nuestra dependencia de Internet, también nuestra libertad, prosperidad y calidad de vida son cada vez más dependientes de una SRI robusta: si falla Internet y, en caso de una urgencia, no se puede acceder por vía electrónica a los historiales médicos, ello conllevará la muerte de gente. En cualquier caso, la seguridad de las infraestructuras críticas de información en Europa está sometida a una amenaza cada vez mayor y nuestro nivel de SRI no es suficientemente bueno.

3.2 El director de Europol afirmo el año pasado estar «(…) enormemente preocupado por esta gran, y desmerecida, confianza en el carácter indestructible de Internet» ([8]). Con frecuencia oímos hablar de nuevos ciberataques a infraestructuras esenciales por parte de delincuentes, terroristas o gobiernos extranjeros. Los objetivos no notifican la mayor parte de estos ataques por temor a dañar su reputación; no obstante, en las últimas semanas hemos asistido a ataques en las infraestructuras de Internet ([9]) y en los sistemas bancarios ([10]) de Europa de tal gravedad que no ha sido posible ocultarlos. Un informe ([11]) cifra en 92 y 82 millones los ciberataques que sufrieron en 2011 los Países Bajos y Alemania respectivamente. El gobierno británico calcula que el Reino Unido sufrió ese mismo año 44 millones de ciberataques, que ocasionaron un coste económico que podría llegar hasta los 30 000 millones de euros ([12]).

3.3 El Consejo de la UE abordó en 2007 el problema de la SRI en Europa ([13]). Sin embargo, el planteamiento político que se viene adoptando desde entonces ([14]) ha confiado principalmente en una actuación voluntaria por parte de los Estados miembros, y son pocos los países que han emprendido acciones eficaces al respecto. El Comité señala que numerosos Estados miembros no han publicado todavía su estrategia nacional en materia de ciberseguridad, ni han elaborado un plan de contingencia para ciberincidentes. Además, algunos de ellos tienen todavía pendiente la creación de un equipo de respuesta a emergencias informáticas (CERT). Por último, algunos Estados miembros siguen sin ratificar el Convenio del Consejo de Europa sobre la Ciberdelincuencia ([15]).

([8]) http://forumblog.org/2012/05/what-if-the-internet-collapsed/
([9]) http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html?pagewanted=all&_r=0
([10]) http://www.dutchnews.nl/news/archives/2013/04/online_retailers_demand_banks.php
([11]) http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011
([12]) UKCyber Security Strategy – Landscape Review: http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf
([13]) Resolución del Consejo 2007/C 68/01.
([14]) COM(2006) 251 y COM(2009) 149.
([15]) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

3.4 Los diez Estados miembros más avanzados en SRI han creado el Grupo de CERT de los gobiernos europeos (EGC) con el ánimo de colaborar estrechamente y dar respuesta a los incidentes en materia de seguridad de las redes y de la información. La admisión a este grupo está cerrada: por el momento, los 17 Estados miembros restantes, menos avanzados en SRI, y el reciente CERT de la UE ([16]) están excluidos de este grupo de élite. Se está abriendo una nueva brecha digital entre los Estados miembros más avanzados en RSI y el resto. Si no se cierra esta brecha, la línea divisoria de la SRI golpeará en el corazón del mercado único digital, limitando los avances en términos de confianza, armonización e interoperabilidad. Además, si no se emprenden acciones decididas, es probable que se agrave esta división entre los Estados miembros más y menos avanzados, con lo que aumentarían también las deficiencias del mercado interior asociadas a los diferenciales de capacidad entre los Estados miembros.

3.5 El éxito de la estrategia de ciberseguridad y la eficacia de la propuesta de Directiva SRI dependerá de la existencia en Europa de un sector fuerte y de un número suficiente de trabajadores especializados en esta materia. El CESE valora positivamente que la Directiva propuesta incluya la necesidad de que los Estados miembros inviertan en educación, concienciación y formación en materia de RSI. El Comité también desearía que todos los Estados miembros llevaran a cabo un esfuerzo especial con vistas a informar, educar y apoyar al sector de las PYME en todo lo relacionado con la ciberseguridad. Las grandes empresas pueden adquirir fácilmente los conocimientos que precisan, pero las PYME necesitan apoyo.

3.6 El CESE aguarda con impaciencia el inicio de su colaboración con la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) para promover la cuestión de la SRI durante el «mes de la ciberseguridad» que tendrá lugar a finales del presente año. Por lo que respecta al objetivo recogido en la Estrategia de ciberseguridad y la directiva RSI de implantar una cultura de concienciación en torno a la seguridad en toda la Unión y de elevar el nivel de cualificación en materia de SRI, el Comité llama la atención de la Comisión sobre las «competiciones de *hackers*» para adolescentes que tantos resultados han dado para sensibilizar en algunos Estados miembros y en los Estados Unidos.

3.7 El Comité también valora positivamente el compromiso contraído en la Estrategia de ciberseguridad acerca del gasto en I+D+i para tecnologías relacionadas con la SRI.

3.8 El aumento de la computación en nube crea un gran número de nuevos peligros de ciberseguridad a los que habrá que hacer frente. Por ejemplo, los delincuentes cibernéticos tienen a disposición en la actualidad una capacidad ingente de computación a un coste relativamente reducido, y la información de miles de empresas se encuentra ahora en almacenes de datos centralizados que son vulnerables a ataques específicos. El CESE ya ha hecho un llamamiento en favor de una mayor resiliencia cibernética para la computación en nube ([17]).

([16]) El CERT de la UE es el equipo permanente de respuesta a emergencias informáticas de las instituciones, agencias y órganos de la UE.

([17]) «La computación en nube en Europa» DO C 24 de, 28.1.2012, p. 40 y «Liberar el potencial de la computación en nube en Europa» DO C 76 de, 14.3.2013, p. 59.

3.9 El Comité ha solicitado anteriormente la introducción de un sistema de identificación electrónica de la UE, de carácter voluntario, para las transacciones en línea como complemento a los sistemas nacionales ya existentes. Este sistema proporcionaría un mayor grado de protección contra el fraude, un mayor clima de confianza entre los operadores económicos, menores costes en la provisión de servicios y una mayor calidad de servicio y de protección para los ciudadanos.

4. **Observaciones específicas**

4.1 Lamentablemente, esta propuesta de Directiva de la Comisión sobre la SRI es demasiado vacilante, carece de la suficiente claridad y depende demasiado de la autorregulación por parte de los Estados miembros. La falta de normas, definiciones claras y obligaciones categóricas, especialmente en el capítulo IV de la Directiva, ofrece a los Estados miembros una excesiva flexibilidad para interpretar y transponer elementos fundamentales de ese documento. Un reglamento que estableciera para los Estados miembros unas obligaciones legales bien definidas sería más eficaz que una directiva.

4.2 El Comité señala que el artículo 6 de la Directiva exige que cada Estado miembro designe una «autoridad competente» para supervisar y contribuir a una aplicación coherente de la Directiva en toda la Unión. Asimismo, se señala que el artículo 8 establece una «red de cooperación», la cual, en virtud de las competencias otorgadas a la propia red y a la Comisión, proporcionará a nivel europeo liderazgo, supervisión, y, si se considera oportuno, verificará su cumplimiento, hasta el nivel de los Estados miembros. El CESE cree que, sobre la base de este marco de gobernanza, la UE debería considerar la creación de una autoridad a nivel de la UE para la seguridad de las redes y de la información, similar a la autoridad central de la industria aeronáutica (EASA), que establece las normas y hace cumplir y respetar las disposiciones de seguridad en aeronaves, aeropuertos y operaciones de líneas aéreas.

4.3 La autoridad de SRI a nivel de la UE que propone el Comité en el punto 4.2 podría crearse basándose en la labor de ciberseguridad que ya han llevado a cabo, entre otros, ENISA, el Comité Europeo de Normalización (CEN), los CERT y el Grupo de CERT de los gobiernos europeos (EGC). Una autoridad de este tipo establecería normas y realizaría un seguimiento de la aplicación de todos los elementos de la SRI, desde la certificación de terminales seguros y su utilización, hasta la seguridad de la red y la seguridad de los datos.

4.4 Dada la gran interdependencia de los Estados miembros a la hora de proporcionar SRI en toda la Unión Europea y los costes elevadísimos que los fallos de seguridad de las redes y la información podrían generar a todas las partes interesadas, el CESE aboga por que, en caso de deficiencias en el cumplimiento, se incluyan en la legislación sanciones explícitas, proporcionadas y armonizadas de manera que reflejen la dimensión paneuropea de la responsabilidad y la magnitud de los daños que pudieran ocasionarse no sólo en el mercado nacional sino, también, en el conjunto de la Unión. El artículo 17 de la Directiva, referente a las sanciones, reviste un carácter general, ofrece un excesivo margen a los Estados miembros para imponer sanciones y no proporciona suficientes orientaciones para tomar en consideración las repercusiones transfronterizas y paneuropeas.

4.5 En la actualidad, los gobiernos y los proveedores de servicios vitales no hacen públicos los fallos de seguridad y resiliencia salvo que estén obligados a hacerlo. Este silencio perjudica a la capacidad de Europa para responder con celeridad y eficacia a las amenazas cibernéticas y mejorar en general la SRI intercambiando conocimientos. El Comité felicita a la Comisión por decidir la obligatoriedad de notificar, en virtud de la Directiva, todos los incidentes significativos en materia de SRI. El CESE considera que la información voluntaria de incidentes no puede funcionar dado que el temor a perder reputación o a tener que asumir responsabilidades incita a silenciar los fallos.

4.6 Sin embargo, el artículo 14 de la Directiva, relativo a la notificación, no define qué constituiría un incidente «que tenga efectos significativos» en la seguridad, y otorga un margen excesivo a las entidades relevantes y a los Estados miembros para notificar o no los incidentes en materia de SRI. Una legislación efectiva exige unos requisitos inequívocos. Como quiera que la propuesta de Directiva es demasiado vaga en una cuestión esencial como es la definición de los requisitos, no es posible hacer responsables a las partes por fallos en el cumplimiento, como se prevé en el artículo 17 de la Directiva.

4.7 Dado que la prestación de la SRI se halla fundamentalmente en manos del sector privado, es importante fomentar un alto grado de confianza y cooperación con todas las empresas responsables de infraestructuras y servicios de información vitales. Se aplaude y elogia, pues, la iniciativa lanzada por la Comisión en 2009 con el nombre de *European Public Private Partnership for Resilience* (EP3R). Sin embargo, el Comité cree que esta iniciativa debe verse reforzada y respaldada por una obligación reglamentaria en la Directiva SRI que fuerce a cooperar a las partes interesadas de importancia clave que no se comprometan adecuadamente.

4.8 Cada Estado miembro debería publicar un directorio en línea de todas las entidades de su jurisdicción a las que afectan los requisitos de seguridad y las obligaciones de notificación de incidentes que se recogen en el artículo 14 de la Directiva. Además de aclarar cómo decidirá cada Estado miembro aplicar las definiciones del artículo 3 de la Directiva, esta transparencia contribuiría a infundir confianza y alentaría una cultura relativa a la gestión de riesgos entre la ciudadanía.

4.9 El CESE observa que los desarrolladores de programas informáticos y los fabricantes de equipos físicos quedan explícitamente excluidos del ámbito de aplicación de la Directiva porque no son proveedores de servicios de la sociedad de la información Sin embargo, el Comité considera que la propuesta de Directiva debería estipular que aquellas entidades a las que el propio acto impone obligaciones deberían poder recurrir contra los proveedores de programas informáticos y de equipos físicos en caso de que sus productos o servicios presentaran algún defecto que coadyuvara directamente a incidentes de SRI.

4.10 Aun cuando la Comisión calcula que la aplicación de la Directiva propuesta en el ámbito de la SRI costará anualmente en torno a los 2 000 millones de euros, repartidos entre los sectores público y privado de Europa, el Comité señala que algunos Estados miembros sometidos a presiones financieras pasarán apuros para encontrar la inversión que exige su cumplimiento. Con vistas al cumplimiento de la SRI, es necesario examinar la manera de ofrecer ayuda en el marco del MFP recurriendo a diversos instrumentos, como el Fondo Europeo de Desarrollo Regional (FEDER) y, posiblemente, el Fondo de Seguridad Interior.

Bruselas, 22 de mayo de 2013.

El Presidente
del Comité Económico y Social Europeo
Henri MALOSSE