Inteligencia Artificial y la Administración de Justicia: SEKT y CAPER

http://cursosextraordinarios.unizar.es/curso/2015/tramitacion-y-comunicacion-electronicas-en-la-administracion-de-justicia

Zaragoza, 23 Octubre 2015

pompeu.casanovas@uab.cat

Crowdsourced crisis mapping: how it works and why it matters

Wednesday, 16 May 2012 05:23

Read the full article by Marta Poblet and Pompeu Casanovas at the Australian website The Conversation.

THE CONVERSATION

The First International Workshop on Artificial Intelligence and e-Discovery: Information Retrieval and Knowledge Management for Legal Discovery Proceedings

Monday, 05 March 2012 12:52

An ECAI 2012 workshop

Legal professionals are used to consuming an important part of their time searching, retrieving and managing legal information. Improving the functionalities for search, retrieval and management of legal documents is

A student's team supervised by Dr. Núria Casellas wins Cornell University's Science Fair

Wednesday, 11 April 2012 10:08

Every year, Cornell's Faculty of Computing and Information Science sponsors a "science fair called Bits on our Minds (BOOM). The exhibition showcases cutting-edge student research in all manner of digital realms, ranging from robotics to information retrieval to social applications to game design. This year, a team of Masters of Engineering students supervised by Dr. Núria Casellas presented their work on Legal Linked Data. The project won a BOOM Sponsor's Award from Susquehanna International Group, a financial trading firm.

PhD position Artificial Intelligence and Forensic Science (Utrecht University)

Monday, 05 March 2012 10:32

This PhD position is part of the project "Designing and Understanding Forensic Bayesian Networks with Arguments and Scenarios" that is funded by the Netherlands Institute for Scientific Research in the Forensic Science program (www.nwo.nl/forensicscience). The project is a cooperation of the University of

IDT Series
Llibre Blanc de la mediació a Catalunya
Erytheis
www.iijlac.org
JOURNAL OF CATALAN INTELLECTUAL HISTORY

Follow us on...
Facebook Page
Google+ Page
Linked In
Twitter

Sumario

- I Introducción
- A *Materiales*
- B *Conceptos*
- *C Modelo regulador*
- II Web 2.0 y Web 3.0
- A *Ejemplo*
- B *Lenguajes*
- *C Linked Open Data (LOD)*
- III La Web Semántica y el Derecho
- A *Dbpedia* (20011-14)- LOGD
- B *CELLAR (2014-15)*
- C *SEKT (2006) -CGPJ*
- *D CAPER (2013) – EU LEAs*
- *D FIPs* (PD, seguridad y cumplimento mediante diseño (PbD)
- IV Conclusiones

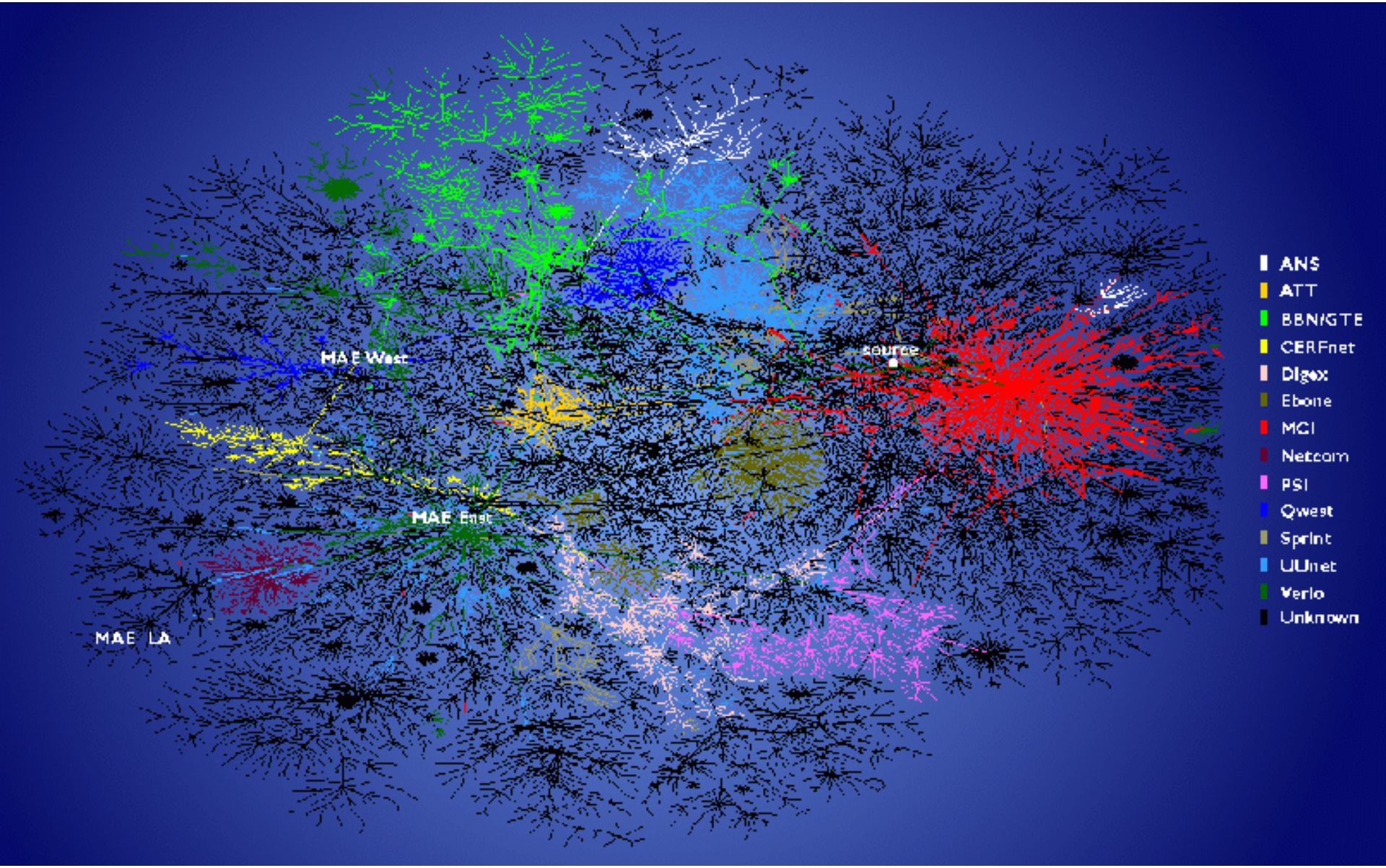
I. INTRODUCCIÓN

MATERIALES I

- 2012. Vallbé, JJ., Fernández-Barrera, M., Casellas, N.; Casanovas, P. (Eds) . *Lecturas de Web Semántica*. Aplicaciones para el derecho en la nueva generación de la red. Granada: Comares.
- "Algunas líneas de investigación en gestión del conocimiento jurídico. Web semántica, ODR y derecho relacional" *SCIRE. Representación y organización del conocimiento. Scire. 18:1 (en.-jun. 2012), pp. 15-28. ISSN 1135-3716.*
- 2014. Casanovas, P. "Tecnología, Inteligencia Artificial y Web Semántica. Un mundo para todos y para cada uno", Jorge Fabra y Álvaro Núñez (eds.) *Enciclopedia de Teoría y Filosofía del Derecho, vol. 1, Cap. 23, Instituto de Investigaciones Jurídicas, UNAM, México, 2014 , México, pp. 815-877. Online: http://biblio.juridicas.unam.mx/libros/libro.htm?1=3796*
- 2014. Casanovas, P. & Barral, I. Ed. Invitados. *Revista Democracia Digital e Governo Eletrônico (Brazil), Sección ODR y XML jurídico (Junio), v. 10: 1 http://www.buscalegis.ufsc.br/revistas/index.php/observatoriodoegov , pp. 400*

MATERIALES II

- 2014 P. Casanovas, P. (with U. Pagallo, M. Palmirani, G. Sartor) (Eds.) *AI Approaches to the Complexity of Legal Systems IV-V. Social Intelligence, Models and Applications for Law and Justice Systems in the Semantic Web and Legal Reasoning*. *rtificial Intelligence, LNAI, Springer Heidelberg NewYork Dordrecht London, Heidelberg, Dordrecht: Springer , 2014. http://link.springer.com/book/10.1007/978-3-662-45960-7*
- 2014. P.C. "Semantic Web Regulatory Models: Why Ethics Matter", *Philosophy and Technology. Special Issue on Information Society and Ethical Inquiries, Philosophy & Technology: Volume 28, Issue 1 (2015), Page 33-55.*
- Pompeu Casanovas : "Conceptualisation of Rights and Meta-Rule of Law for the Web of Data" . *Democracia Digital e Governo Eletrônico, v. 1, n. 12 (2015): 18-41.* http://buscalegis.ufsc.br/revistas/index.php/observatoriodoegov/issue/view/250



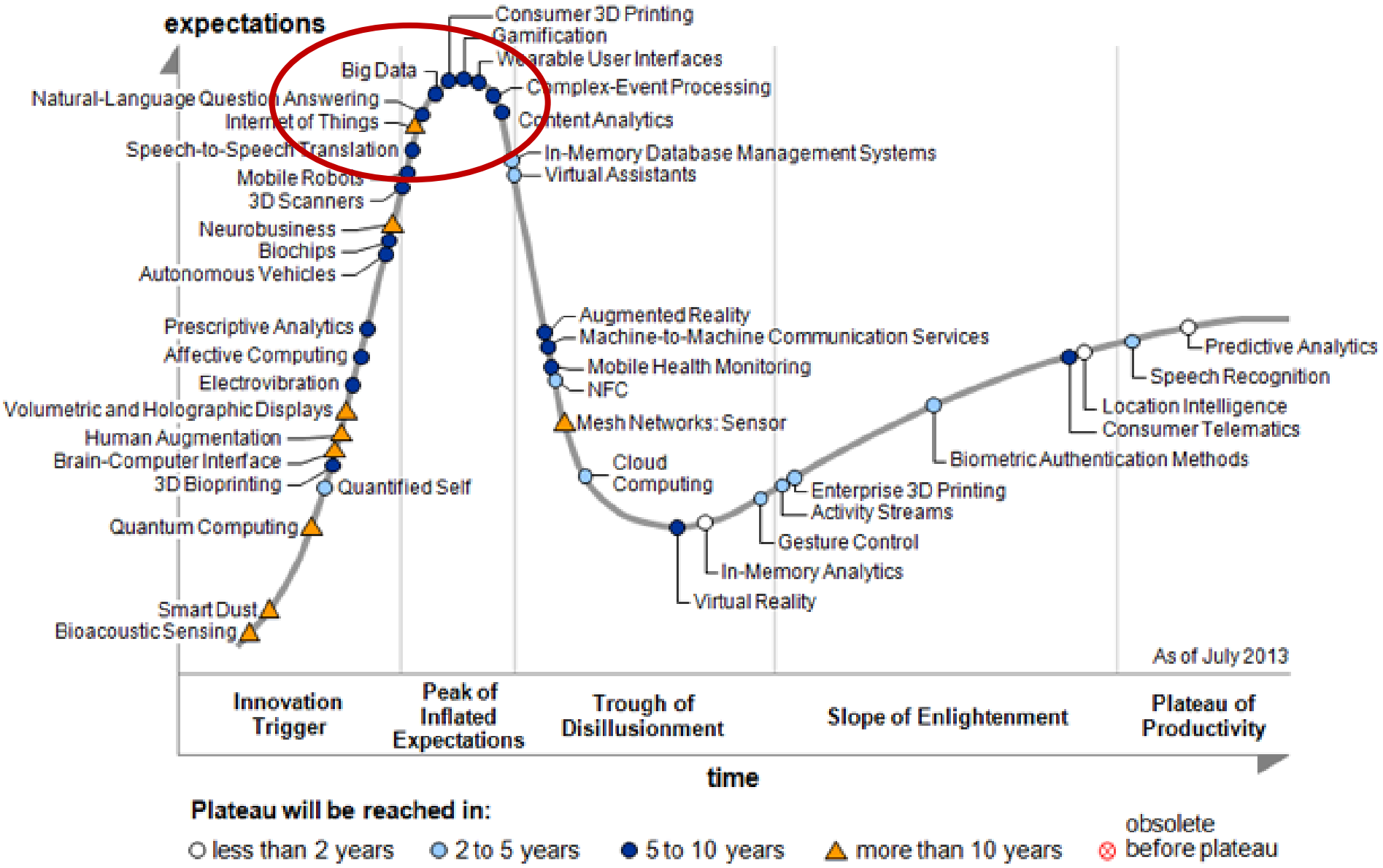
kitter data depicting a macroscopic snapshot of Internet connectivity,
with selected backbone **ISP**s (Internet Service Provider) colored separately

By **K. C. Claffy** email: kc@caida.org

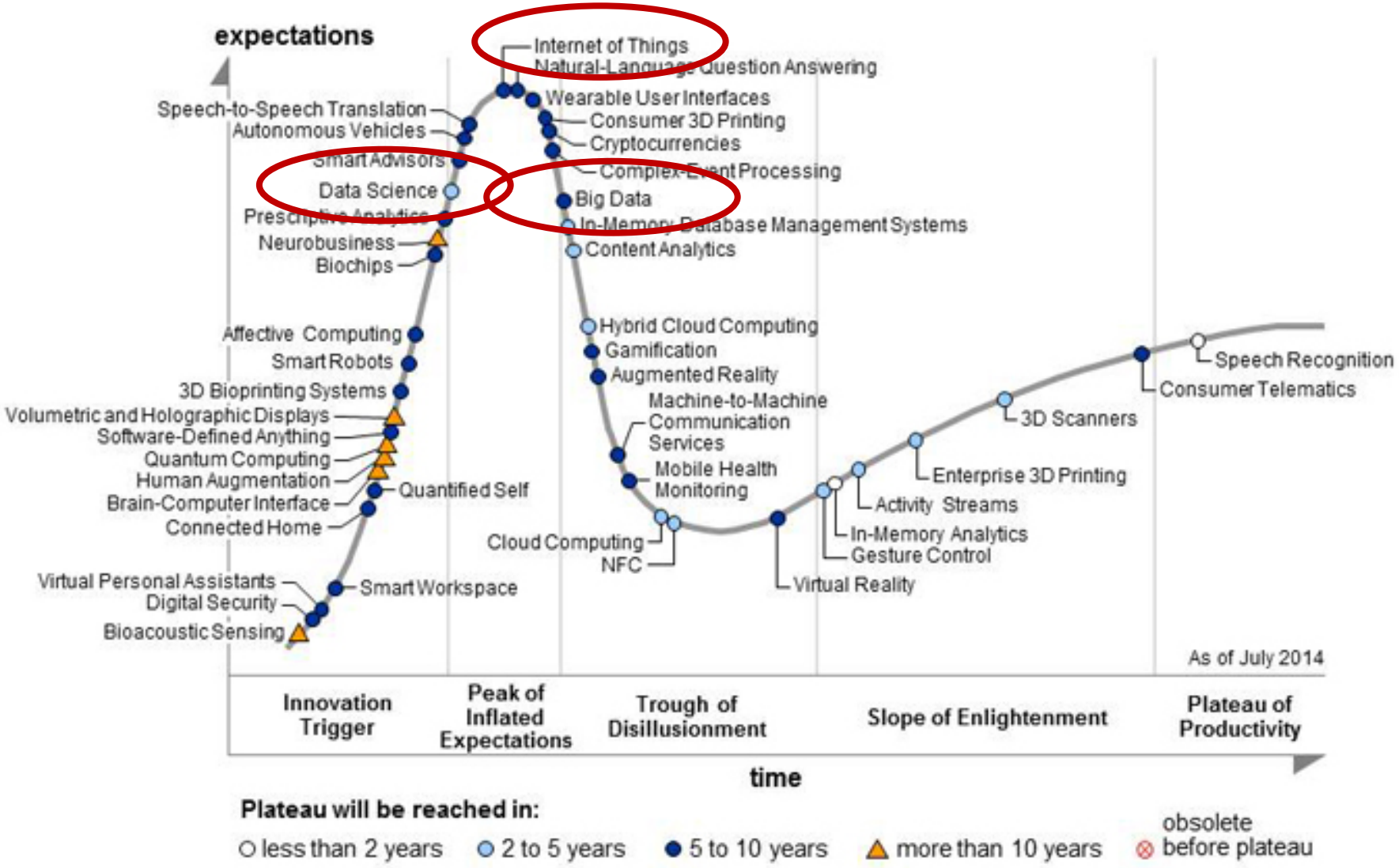
http://www.caida.org/publications/papers/bydate/index.xml

Gigabytes de Datos

- 30.000 gigabytes de datos por segundo (1 gigabyte= 10^9, 1.000 000.000 bytes)
- Twitter genera diariamente 500 millornes de tuits. Ahora somos capaces de procesar y analizar 50 millones de tuits por día, mediante extracción de patrones y esquemas de información (“memes”).
- Pero...el Gartner *Hype Cycle for Emerging Technologies* (2014-15) ya no situa el *big data* en la cima de expectaciones emergentes, sino en los bordes de las tecnologías conocidas, pero aún inmaduras.



Gartner 2013: featuring the relationship between humans and machines due to the increased hype around smart machines, cognitive computing and the Internet of Things.



http://www.gartner.com/newsroom/id/2819918

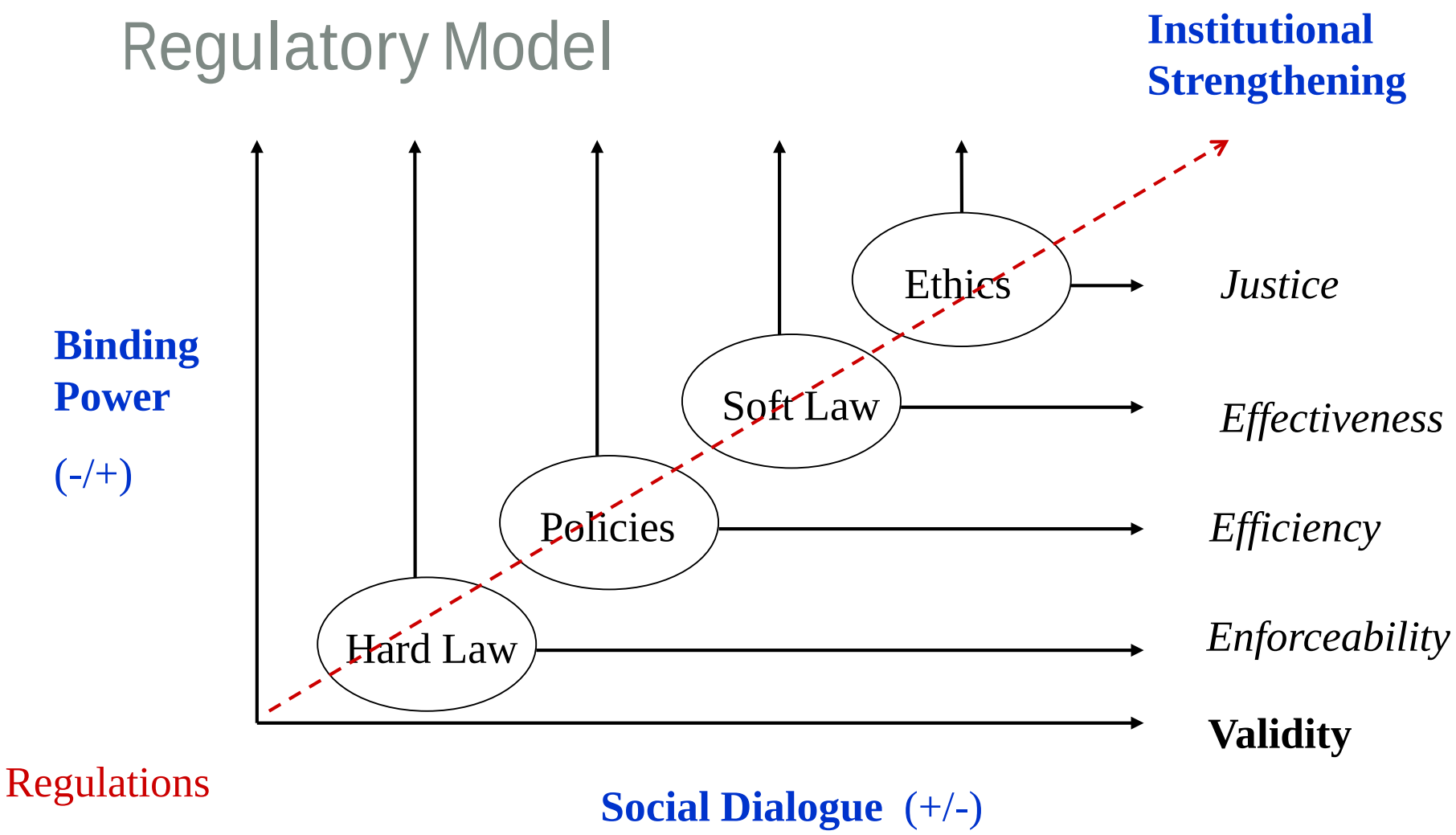
Conceptos I

- Legal Crowdsourcing: Producción agregada de conocimiento jurídico
- Legal Open Data (Datos abiertos vinculados o enlazados): Vínculo semántico de datos jurídicos a través de “metadatos” (Standards XML)
- Derecho Relacional: Vínculo de conexión entre la Web 2.0 (web social) y la Web 3.0 (web de datos), basado en la confianza (*trust*), en la arquitectura (diseño institucional) y en el diálogo como fuente de derecho.

Conceptos II

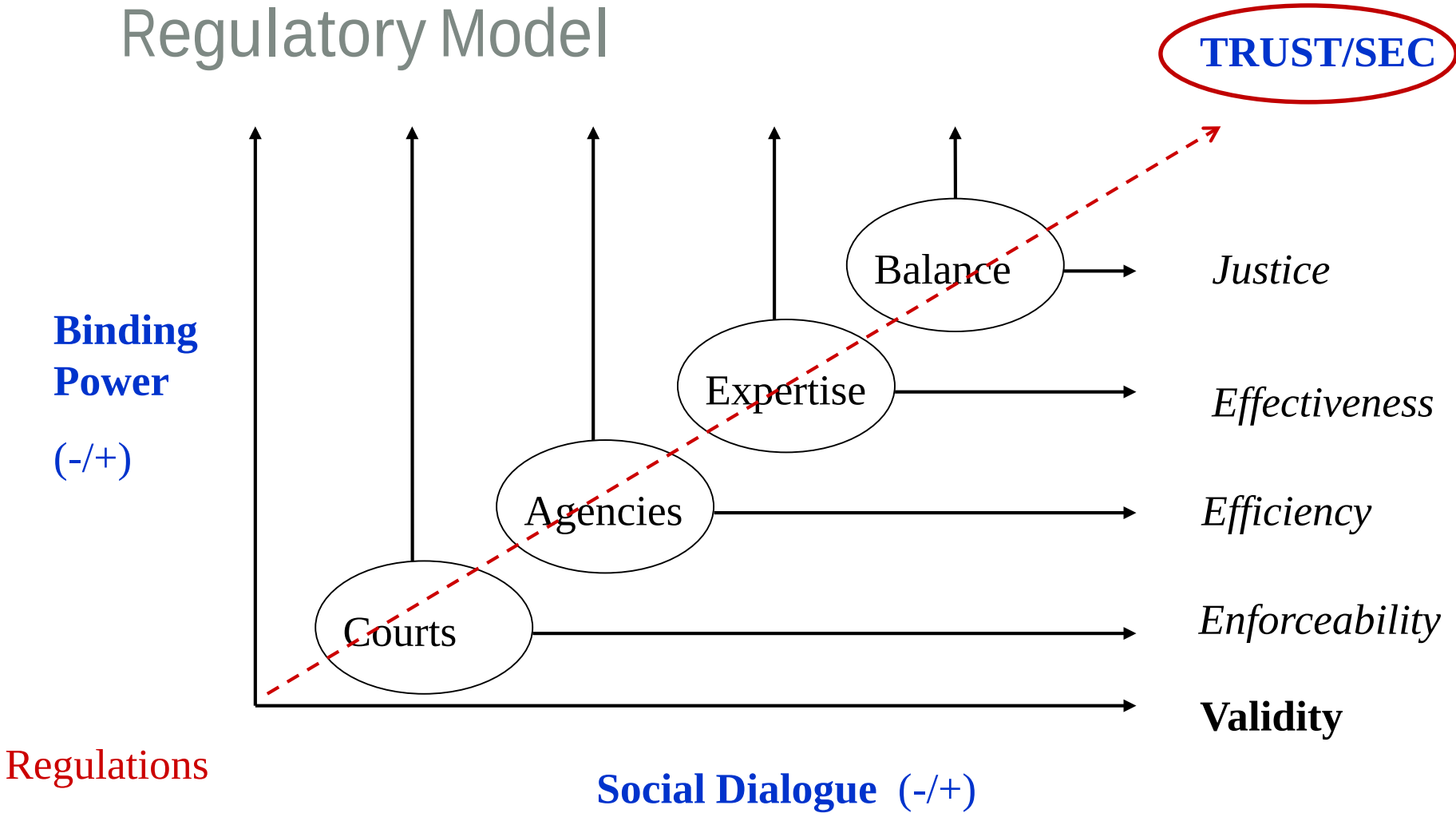
- Sistema regulativo: *ecosistema* o conjunto de comportamientos individuales, colectivos o coordinados (naturales o artificiales) que pueden ser descritos mediante reglas, valores y principios que constituyen su estructura regulativa (‘derecho’)
- Modelo regulador: un diseño de sistema regulativo en el que un núcleo de derecho duro (*hard law*), derecho suave (*soft law*), políticas (*policies*), y ética pueden ser combinados en diferente grado en un conjunto de guías implícitas o explícitas para la interoperabilidad de los sistemas (lenguajes) y la interoperatividad de los agentes (actores).
- La validez puede ser conceptualmente definida como una *propiedad de segundo orden*, un 4-tuplo de ética (justicia), políticas (eficiencia), derecho suave (efectividad) y derecho fuerte (obligatoriedad), en una dimensión de reforzamiento institucional (*institutional strengthening*) —la organización coordenada de componentes que aplican tecnologías semánticas en plataformas determinadas.

Regulatory Model



Continuum of legal institutional strengthening

Regulatory Model



Continuum of legal institutional strengthening

Propiedades de primer orden

- ***Eficiencia*** es un indicador social de buen gobierno que se refiere a la calidad del resultado producido
- ***Efectividad*** es un indicador que indica la relación entre los resultados obtenidos y los recursos utilizados (coste).
- ***Coerción*** se refiere a la posibilidad de acudir a los tribunales para obtener una sentencia y su ejecución
- ***Justicia*** es el resultado de un juicio o auditoría éticos (DPIA ético)

II. WEB 2.0 y WEB 3.0

Fox-trott from Italy - Vivere!, 1937 - YouTube - Mozilla Firefox

Edit View History Bookmarks Tools Help

Fox-trott from Italy - Vivere!, 1937 - Yo...

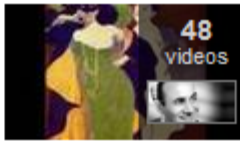
www.youtube.com/watch?v=xYtDtcw4Jbw

YouTube ES

http://www.youtube.com/watch?v=xYtDtcw4Jbw

Upload

GUIDE



Fox-trott from Italy - Vivere!, 1937

240252 · 1,893 videos

Subscribe 11,687

63,355

160 4

Like

About Share Add to

WEB

- Web 1.0: Internet
- Web 2.0: Expresividad (*Tags*): Flikr, YouTube, Wikipedia, Facebook…
- Web 3.0: Expresividad + Semántica (web de objetos vinculados – ”enlazados” – y ya no páginas web)

World Wide Web

- I Web 1.0: Una canción vinculada a mi (usuario) como ***documento***
- II Web 2.0 (e.g. Social Web Social, e.g. YouTube, Twitter): usuarios vinculados por la canción, que añaden y comparten su conocimiento a través de una ***red interactiva***
- III Web 3.0 (e.g. Web de Datos, e.g. DBpedia): la canción misma como objeto semántico que ***se estructura y enlaza como dato*** a otros objetos semánticos.

Web 2.0 (2011)

- ***Comentarios***: *#Thanks for posting this inspiring song. To live without melancholy...laughing at the world's follies...good advice. Nice pictures, too. Many fine designers worked in Italy during the 30s. I especially liked the Fiats going up Mt. Fiat*
- *# □ F.I.A.T = Fabbricazione Italiana Automobile Torino - Automobile Made (in) Torino - Italy*
- *# ora è diventata F:E.A.T., fabbricazione ebraica automobili torino con gli ELKANN* [etc...]
- ***Comentarios eliminados (PD)***: ***Non ti vergogni ad essere in vita e ad avere un cervello che si alimenta creando poi questi malsani pensieri?***
- ***La madre dei deficenti é sempre incinta… la storia insegna purtroppo***

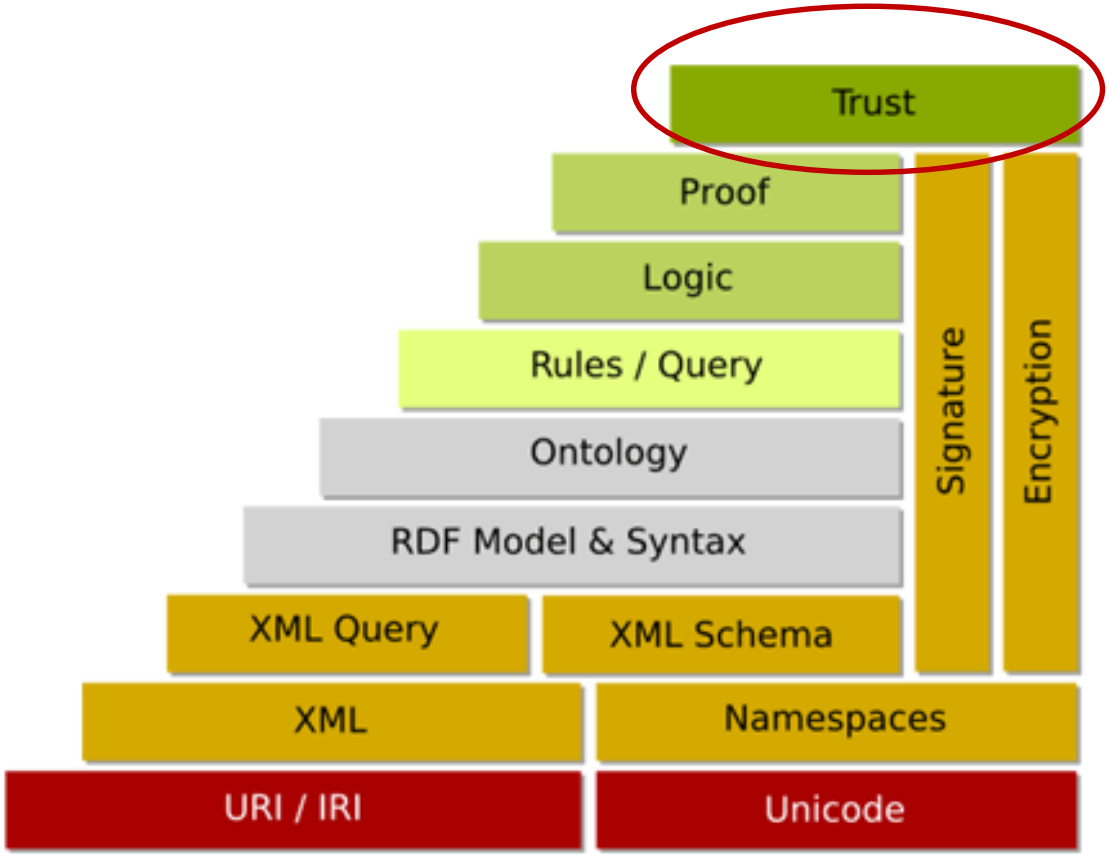
EU: Área de Libertades, Seguridad y Justicia (AFSJ)

- *Reglamento de Protección de Datos Generales* (GDPR) que reemplazará a la Directiva de Protección de Datos 95/46/EC33;
- + *Directiva de Protección de Datos de la Policía y Justicia Penal, que sustituye a la Decisión Marco* 2008/977/JHA. [*Area of Freedom, Security and Justice* (AFSJ)]
- Críticas: fragmentación de AFSJ, "mosaico jurídico" [*legal patchwork*], política errática o no homogénea, juridicciones múltiples, lenguaje no unificado, falta de coordinación

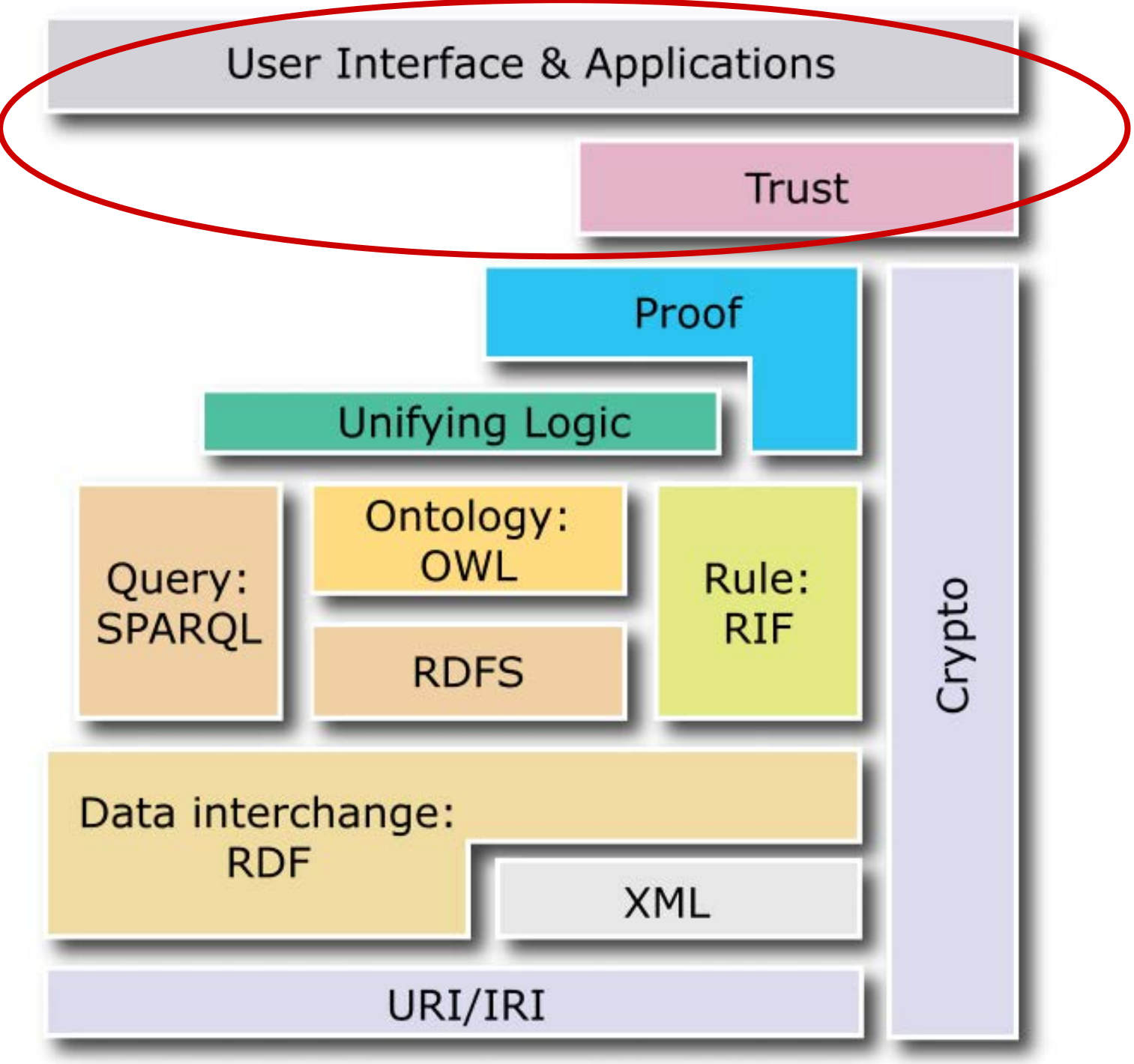
Principios de Privacidad mediante Diseño (PbD) [Cameron-Cavoukian][6]	Principios de Práctica Justa de Información (GPS) [Cavoukian]	Principios Extendidos [Cavoukian]	Principios de la Web Semántica y LOD (Datos Vinculados) [Berners-Lee Hendler][7]	Principios de los Institutos de Información Jurídica [Greenleaf-Bruce][8]	Principios de ODR [Lodder-Zeleznikow-Bellucci][9]	Principios de Crowd-sourcing [Bott-Young][10]	Principios de Crisis Mapping [Poblet-Meier][11]
1. Proactivos, no reactivos; Preventivos, no retributivos		Métodos para **reconocer** la pobreza de diseño en privacidad, para su **prevención** en prácticas y resultados, y para corregir su impacto negativo	URIs para denotar cosas, HTTP **Desreferencia** Formatos serializados Modelado proactivo: XML, RDF, SPARQL, OWL Interconectividad	Inversión en tecnología. Libre acceso al derecho y a la información jurídica	Voluntad de negociar de forma equitativa	Participación Trabajo colaborativo en la gobernanza y toma de decisiones	Presentación de informes Participación proactiva Prevención de conflictos y gestión de crisis y desastres
2. Privacidad como configuración por defecto	3.Especificación del motivo 4.Limitación del registro, datos mínimos 5.Conservación por el usuario. Divulgación limitada	La privacidad se convierte en condición principal, sin que el interesado deba pedir por ella -no se requiere acción alguna.	Desreferencia Accesibilidad Intercambio seguro de datos, protección, almacenamiento, metadatos, ontologías, sistemas de alarma, confianza	**Republicación** Anonimización	**Equidad-** Facilitar la detección de filtraciones de información	**Confianza:** limitación de revelaciones	Vecindad digital **No causar daño**
3. Privacidad incorporada en el diseño		Programa sistémico o metodología para asegurar la **integración** completa de la privacidad en operaciones validables basadas en estándares.	Desreferencia Cuidado de los datos Dtos estructurados Metadatos, Almacenamiento, Enriquecimiento Ontologías nucleares y de dominio, reglas y principios	**Reedición** Reusabilidad Autenticación (Versiones autentificadas) Integridad	**Equidad-** Negociar al amparo de la ley y el uso de BATNAs	**Confianza:** empodera-miento individual y colectivo	GIS monitoriza-ción, implementa-ción de la vecindad digital
4. Funcionalidad plena, de suma positiva y no de de suma cero		Soluciones multifuncionales: intereses y objetivos legítimos de no privacidad, articulación de funciones, métricas según lo acordado	Ciencia de la red, universalidad, datos vinculados, grafo humano gigante, ontologías, desarrollo integral de la Web Semántica	Equilibrio de intereses (editorial/ estado/ usuarios)	**Equidad--** facilitar la detección Enabling Discovery (Privacy Limitation)	**Confianza::** interés agregado, monitoriza-ción, métricas	Confianza: - valores e intereses agregados; monitoriza-ción de procesos, métricas
5. Seguridd integral. Protección completa de todo el ciclo de vida	7. Seguridad		Participación segura Sostenibilidad de las ontologías, vínculo con folksonomías	Integridad, Seguridad, Mantenimiento	Entorno seguro (4a y 5a partes)	Integrity: secure environment and participation	**Seguridad y protección** de de los voluntarios
6. Visibilidad, Transparencia, Mantenimiento abierto.	2.Rendición de cuentas (responsabilidad) 8. Apertura 10.Cumplimiento		**Transparencia Rendición de cuentas** Valor del contenido, anotación y enriquecimiento semántico	Rendición de cuentas, autoridad distribuida de los materiales reeditados	Desarrollo de la transparen-cia	**Confianza:** Transparen-cia	Validación Transparen-cia
7. **Respeto** por la privacidad del usuario. Dirección al usuario	1.**Consentimiento** 6. Precisión 9. Acceso		Personalización Sistemas dirigidos al usuario	**Personalización** Sistemas dirigidos al usuario	Precisión	Valor agregado	**Información veraz y precisa**

Tabla 2. Comparación entre FIPs, PbD, LOD, LII, ODR, principios de *crowdsourcing* y de *crisis mapping*

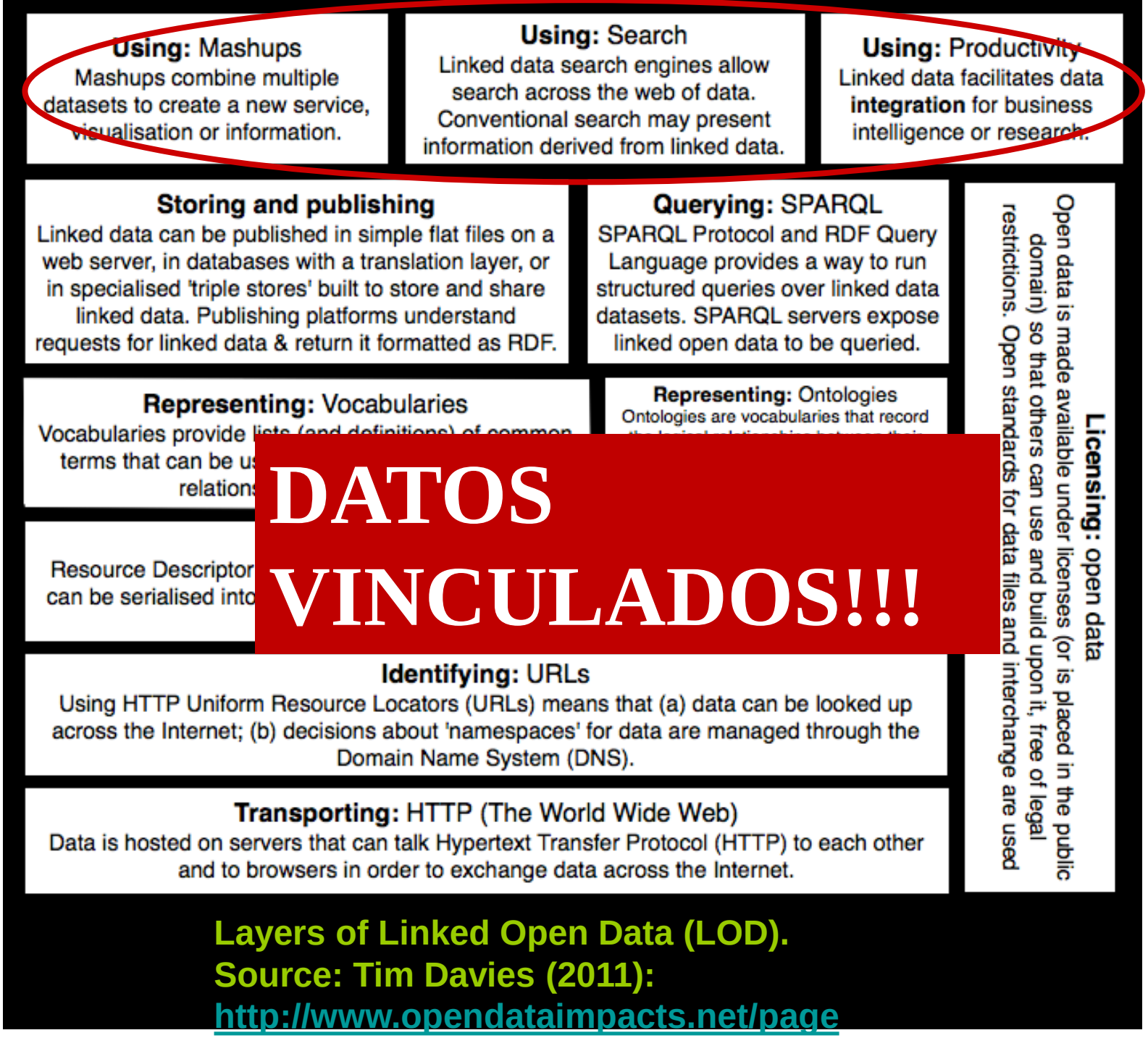
Web Semántica



Berners-Lee's SW stack of languages. Cody Burleson (2007).



Capas de la WS (segunda versión) (T. Berners-Lee). S. Bratt, 2007. W3C http://www.w3.org/2007/03/layerCake.png



Layers of Linked Open Data (LOD).
Source: Tim Davies (2011):
http://www.opendataimpacts.net/page

Vincularlo todo!

- De los datos (LOD) a la gente (GGG)
- De lo local a lo global (Crowdsourcing)
- De la forma al contenido (SW: lenguajes XML, Reglas ML…)
- De los lenguajes de WS a los conceptos regulativos (arquitectura)

LOD (T.Berners-Lee, 2006)

- Usar URIs como nombres de cosas
- Usar HTTP URIs para que la gente pueda incrementar y mejorar estos nombres.
- Cuando alguien enriquece un URI, proporciona información útil utilizando los standards (RDF, SPARQL)
- Incluir vínculos a otras URIs, para que puedan descubrirse más cosas.

De la Web de Datos a la Web de Gente! (2007)

- “There are cries from the heart (e.g The Open Social Web Bill of Rights for my friendship, that relationship to another person, to transcend documents and sites. There is a “Social network Portability” community. It’s not the Social Network *Sites* that are interesting —it is the Social Network itself. The Social Graph. ***The way I am connected, not the way my Web pages are connected*** [emphasis added]. We can use the word *Graph*, now, to distinguish from *Web*. I called this graph the Semantic Web, but maybe it should have been **Giant Global Graph**!”[1]

  [1] Tim Berners-Lee, ‘The Giant Global Graph’, Wed, 2007-11-21, Semantic Web Technologies,
- http://dig.csail.mit.edu/breadcrumbs/node/215

Lenguajes de la WS (Wikipedia!)

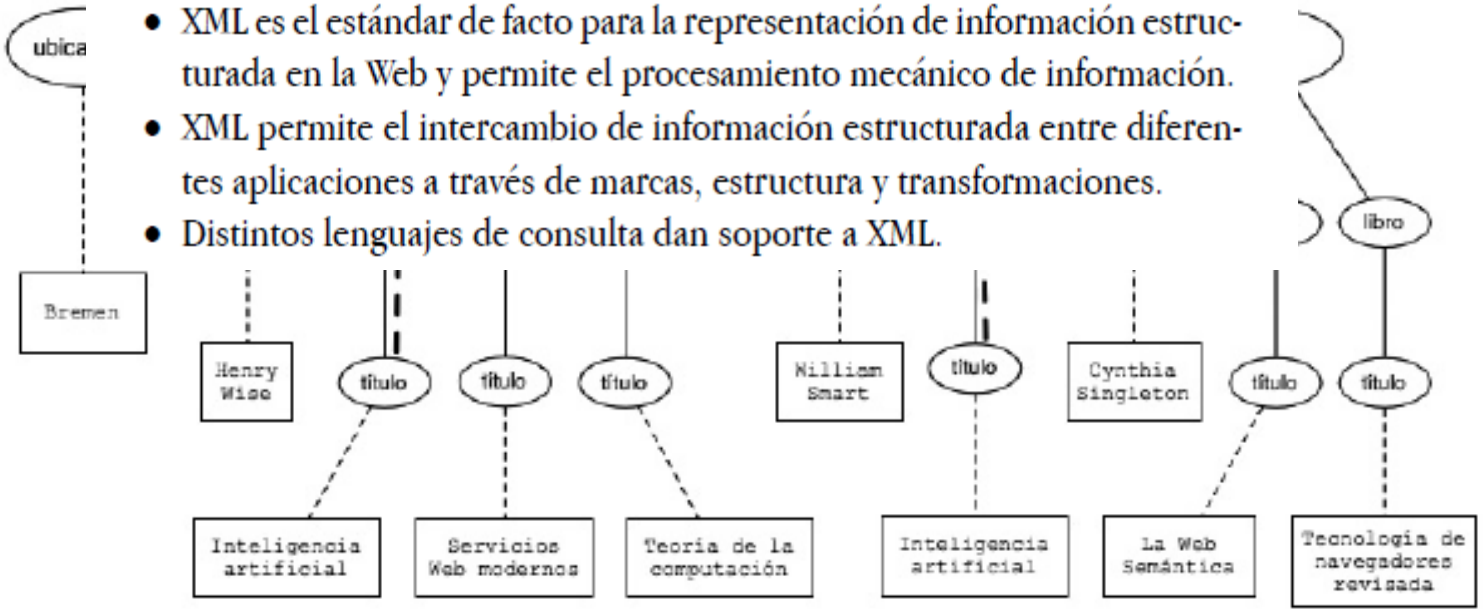
- **XML** aporta la sintaxis superficial para los documentos estructurados, pero sin dotarles de ninguna restricción sobre el significado.
- **XML Schema** es un lenguaje para definir la estructura de los documentos XML.
- **RDF** es un modelo de datos para los recursos y las relaciones que se puedan establecer entre ellos. Aporta una semántica básica para este modelo de datos que puede representarse mediante XML.
- **RDF Schema** es un vocabulario para describir las propiedades y las clases de los recursos RDF, con una semántica para establecer jerarquías de generalización entre dichas propiedades y clases.
- **OWL** es un lenguaje para definir ontologías mediante la descripción detallada de propiedades y clases: tales como relaciones entre clases (p.ej. disyunción), cardinalidad (por ejemplo "únicamente uno"), igualdad, tipologías de propiedades más complejas, caracterización de propiedades (por ejemplo simetría) o clases enumeradas.
- **SPARQL** es un lenguaje de consulta de conjuntos de datos RDF. Además en dicha especificación también se incluye un formato XML que detalla el modo en el que se estructuran los resultados obtenidos.

Metadatos

```
<empresa>
  <tratamientoOfrecido>Fisioterapia</
      tratamientoOfrecido>
  <nombreEmpresa>Centro de Fisioterapia Agilitas</
      nombreEmpresa>
  <personal>
    <terapeuta>Lisa Davenport</terapeuta>
    <terapeuta>Steve Matthews</terapeuta>
    <secretaria>Kelly Townsend</secretaria>
  </personal>
</empresa>
```

XML

- XML es un metalenguaje que permite a los usuarios definir marcas para sus documentos a través del uso de etiquetas.
- La anidación de etiquetas añade estructura a los documentos, y ésta se puede implementar mediante el uso de los esquemas o las DTD.
- XML separa el contenido y la estructura del formato.
- XML es el estándar de facto para la representación de información estructurada en la Web y permite el procesamiento mecánico de información.
- XML permite el intercambio de información estructurada entre diferentes aplicaciones a través de marcas, estructura y transformaciones.
- Distintos lenguajes de consulta dan soporte a XML.



RDF

- RDF ofrece una base para la representación y el procesamiento de metadatos.

El lenguaje de consulta SPARQL se basa en la correspondencia de patrones de grafos. El patrón de grafos más simple es el patrón de la tripla, que es similar a una tripla RDF pero con la posibilidad de tener una variable en las posiciones del sujeto, predicado u objeto, en lugar de un término RDF. La combinación de patrones de triplas nos ofrece un patrón de grafos básico, donde se requiere una correspondencia exacta con un grafo para completar un patrón.

- RDF Schema es un lenguaje de ontologías primitivo, que ofrece algunas primitivas de modelado con significado fijo. Los conceptos clave de RDF Schema son la clase, las relaciones de subclase, la propiedad, las relaciones de subpropiedad, y las restricciones de dominio y de rango.
- Existen distintos lenguajes de consulta para RDF y RDFS, y uno de ellos es SPARQL.

Las clases y las relaciones de subclase de este ejemplo aparecen en la figura 4.6.

```
<rdf:RDF
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-
      ns#"
  xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
  xmlns:owl ="http://www.w3.org/2002/07/owl#"
  xmlns="http://www.cs.vu.nl/~frankh/spool/impresora
      owl#">

<owl:Ontology rdf:about="">
  <owl:versionInfo>
    Mi ejemplo, versión 1.2, 17 de octubre de 2002
```

- OWL es el estándar propuesto para las ontologías Web. Permite describir la semántica del conocimiento de forma accesible para una máquina.
- OWL se construye sobre RDF y RDF Schema y utiliza la sintaxis de RDF, basada en XML. Las instancias se definen utilizando descripciones RDF y se usan la mayor parte de primitivas de modelado RDFS.
- La correspondencia de OWL con la lógica ofrece una semántica formal y soporte al razonamiento. Para esta correspondencia se usan tanto la lógica de predicados como la lógica descriptiva.

```
  </rdfs:comment>
  <rdfs:label>Dispositivo</rdfs:label>
  <rdfs:subClassOf rdf:resource="#producto"/>
</owl:Class>

<owl:Class rdf:ID="productoHp">
  <rdfs:comment>
   Los productos HP son exactamente aquellos productos
   fabricados por Hewlett Packard.
  </rdfs:comment>
  <owl:intersectionOf rdf:parseType="Collection">
    <owl:Class rdf:about="#producto"/>
    <owl:Restriction>
      <owl:onProperty rdf:resource="#fabricado_por"/>
      <owl:hasValue rdf:datatype="&xsd;string">
        Hewlett Packard
      </owl:hasValue>
    </owl:Restriction>
```

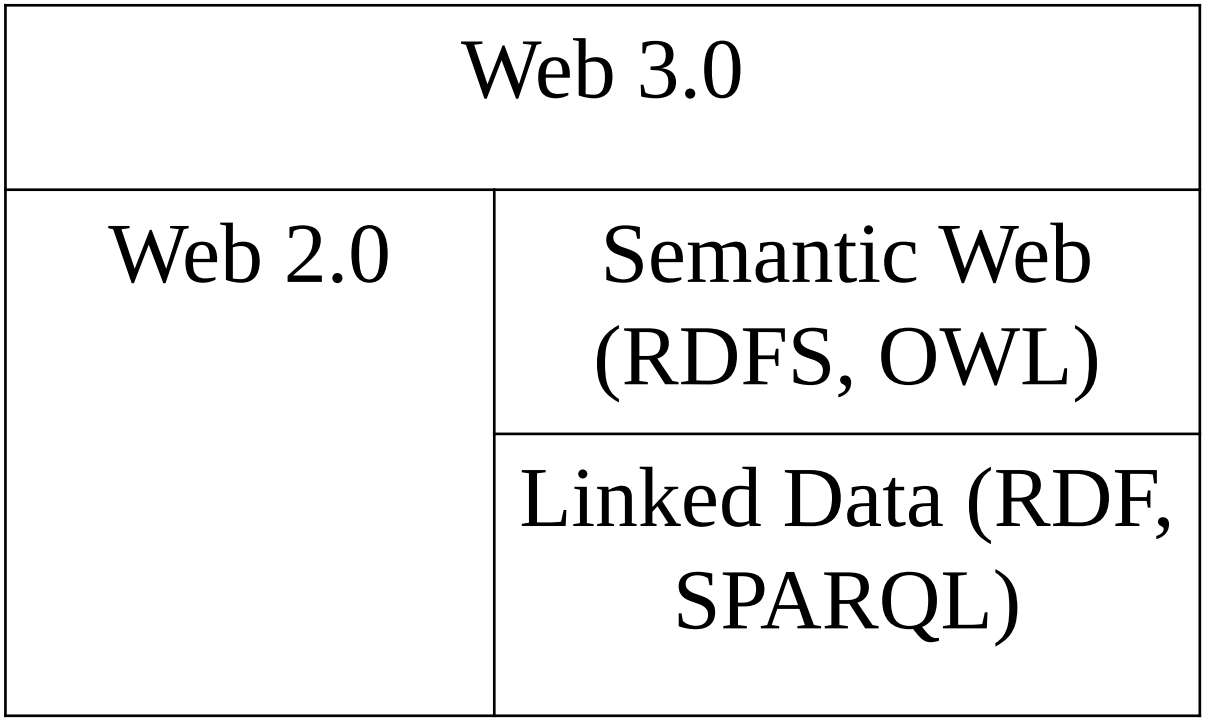


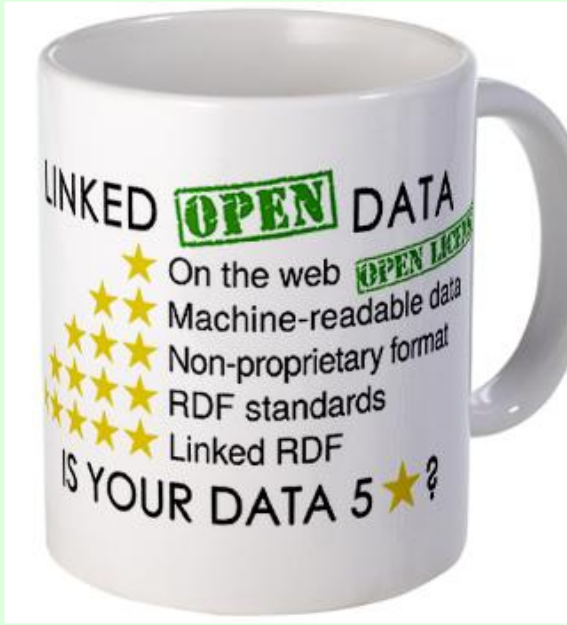
Diagrama de J. HENDLER (2009)

III. WEB SEMÁNTICA Y DERECHO

ed Data - Design Issues - Mozilla Firefox
Edita Visualitza Historial Adreces d'interès Eines Ajuda
d Data - Design Issues
www.w3.org/DesignIssues/LinkedData.html
Google + Flip

Tim Berners-Lee
Date: 2006-07-27, last change: $Date: 2009/06/18 18:24:33 $
Status: personal view only. Editing status: imperfect but published.
Up to Design Issues

Linked Data



The Semantic Web isn't just about putting data on the web. It is about making links, so that a person or machine can explore the web of data. With linked data, when you have some of it, you can find other, related, data.

Like the web of hypertext, the web of data is constructed with documents on the web. However, unlike the web of hypertext, where links are relationships anchors in hypertext documents written in HTML, for data they links between arbitrary things described by RDF,. The URIs identify any kind of object or concept. But for HTML or RDF, the same expectations apply to make the web grow:

1. Use URIs as names for things
2. Use HTTP URIs so that people can look up those names.
3. When someone looks up a URI, provide useful information, using the standards (RDF*, SPARQL)
4. Include links to other URIs. so that they can discover more things.

Simple. In fact, though, a surprising amount of data isn't linked in 2006, because of problems with one or more of the steps. This article discusses solutions to these problems, details of implementation, and factors affecting choices about how you publish your data.

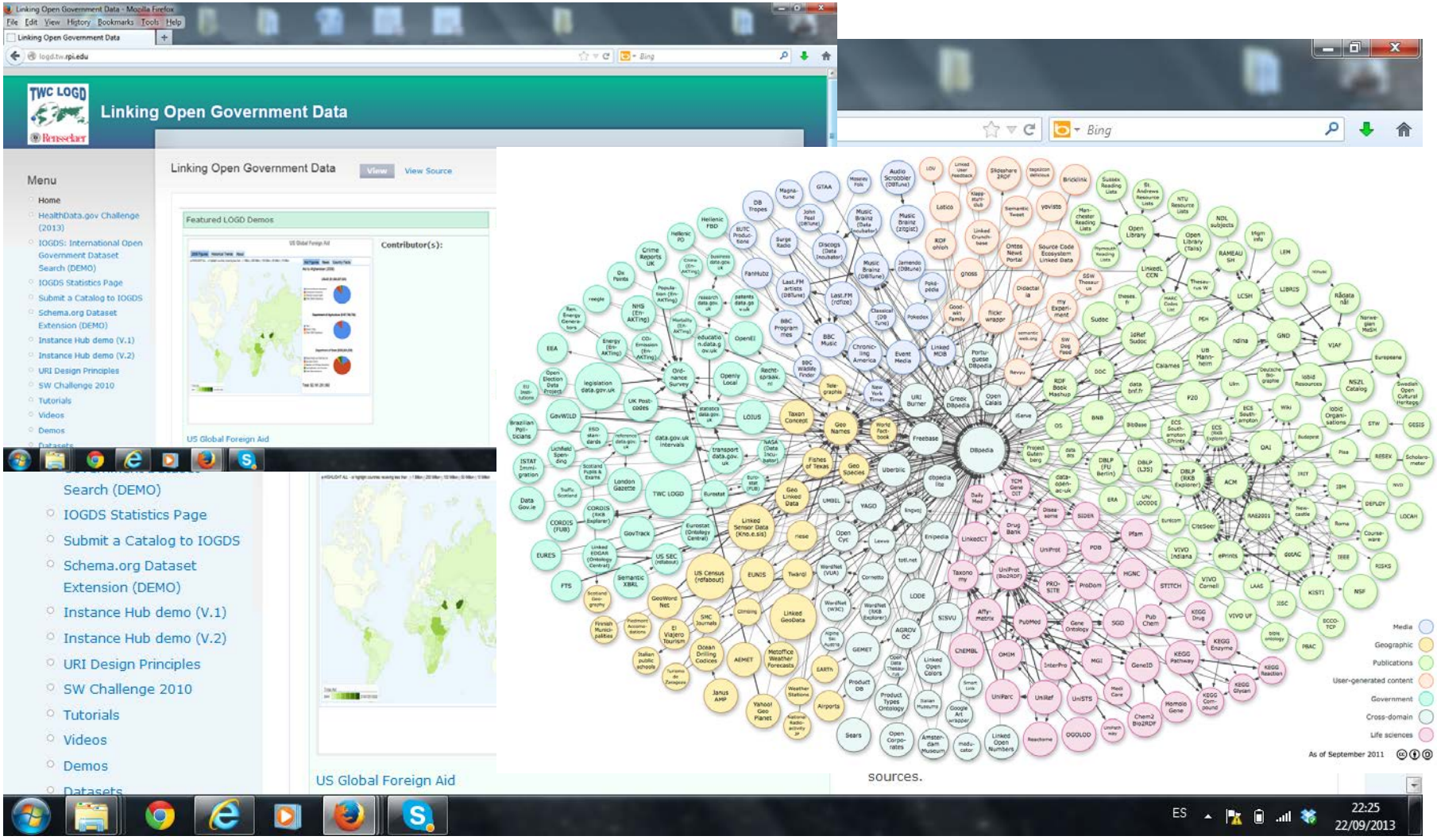
The four rules

I'll refer to the steps above as rules, but they are expectations of behavior. Breaking them does not destroy anything, but misses an opportunity to make data interconnected. This in turn limits the ways it can later be reused in unexpected ways. It is the unexpected re-use of information which is the value added by the web.

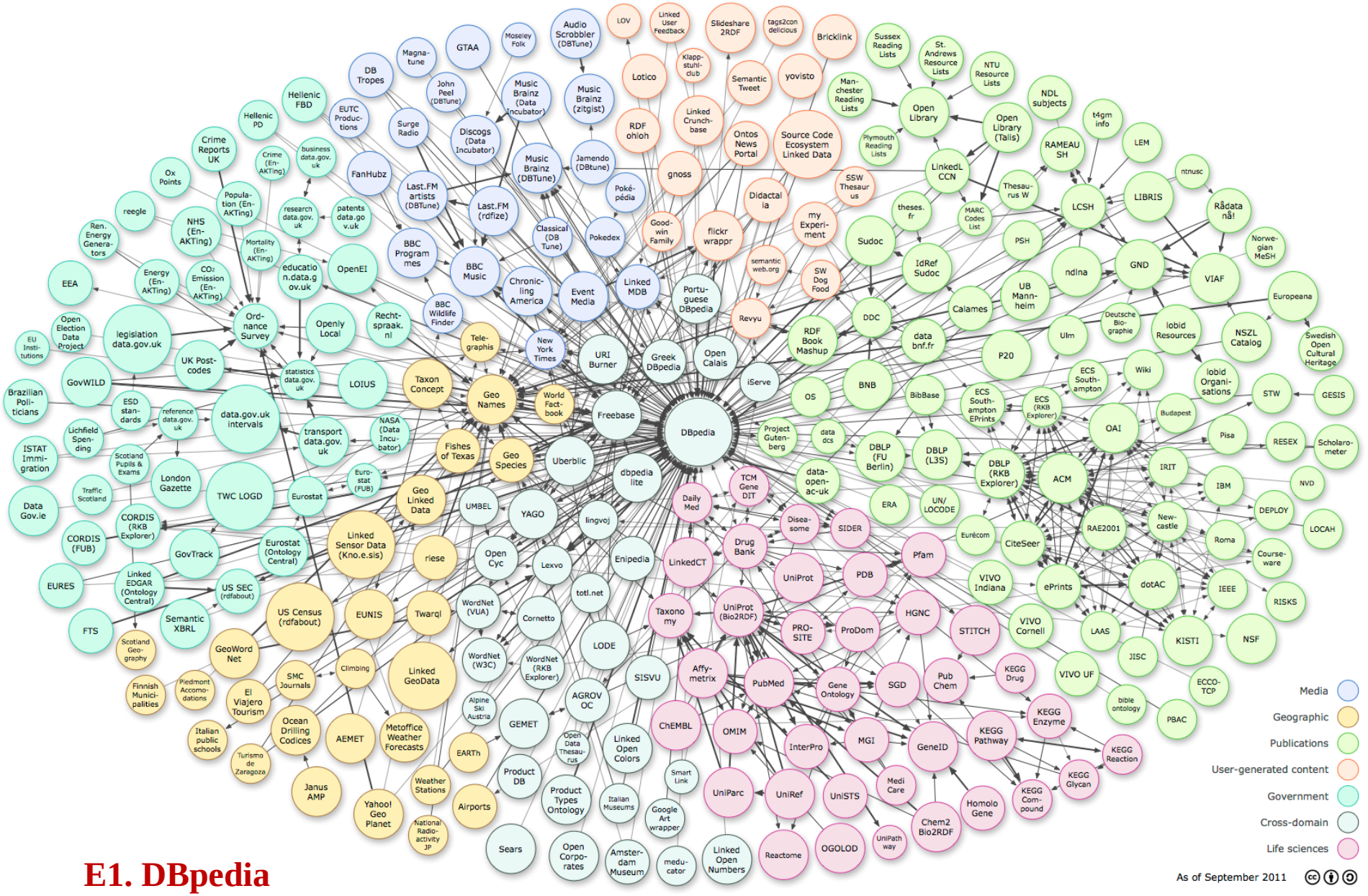
The first rule, to identify things with URIs, is pretty much understood by most people doing semantic web technology. If it doesn't use the universal URI set of symbols, w

icia
Cornell-October-2012-3
Invitation to the Prog...
GeoConsum - Android...
el pais - Google Searc...
Linked Data - Design ...

Web Semántica y Linked Open Government Data (LOGD)

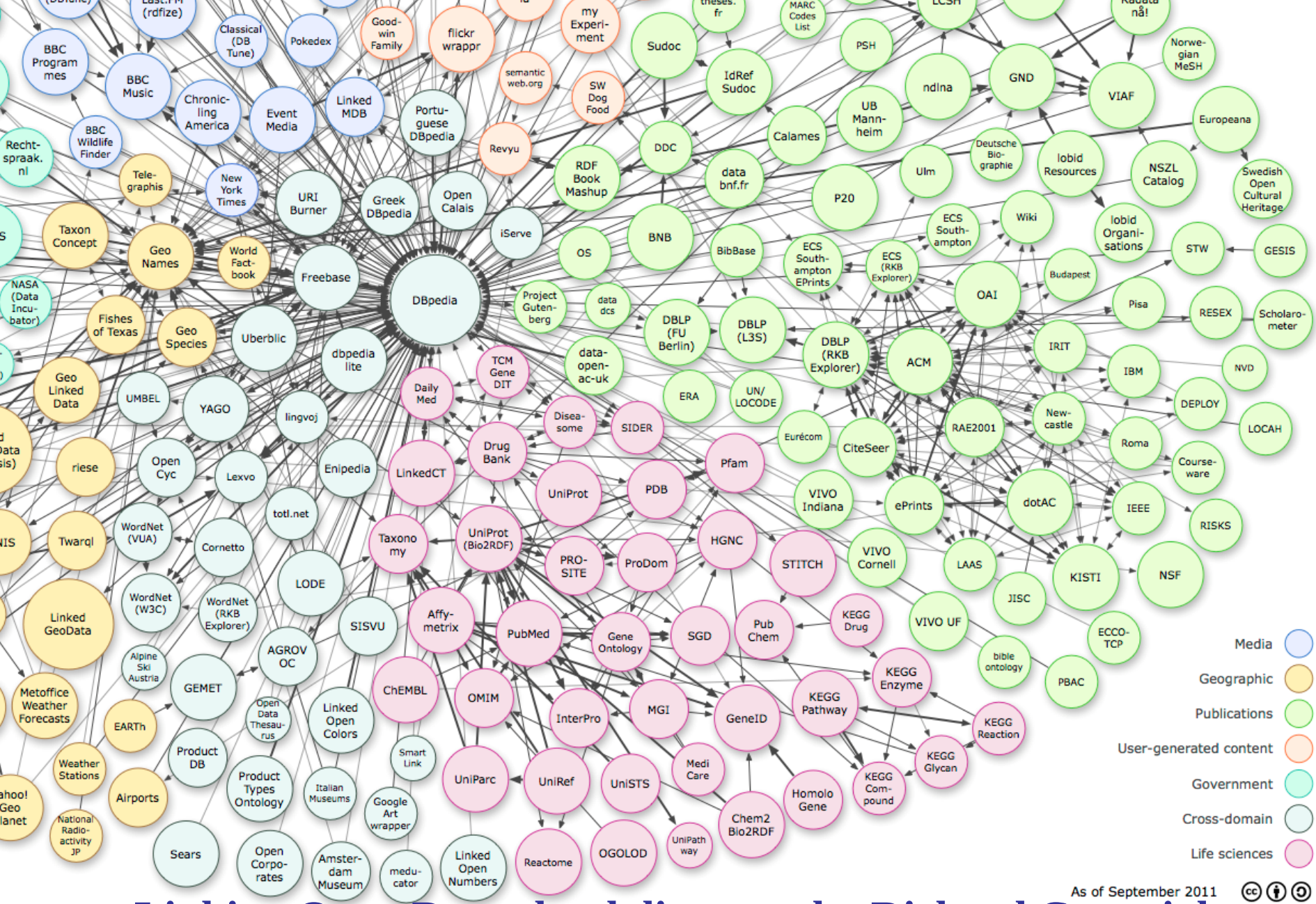


http://logd.tw.rpi.edu/



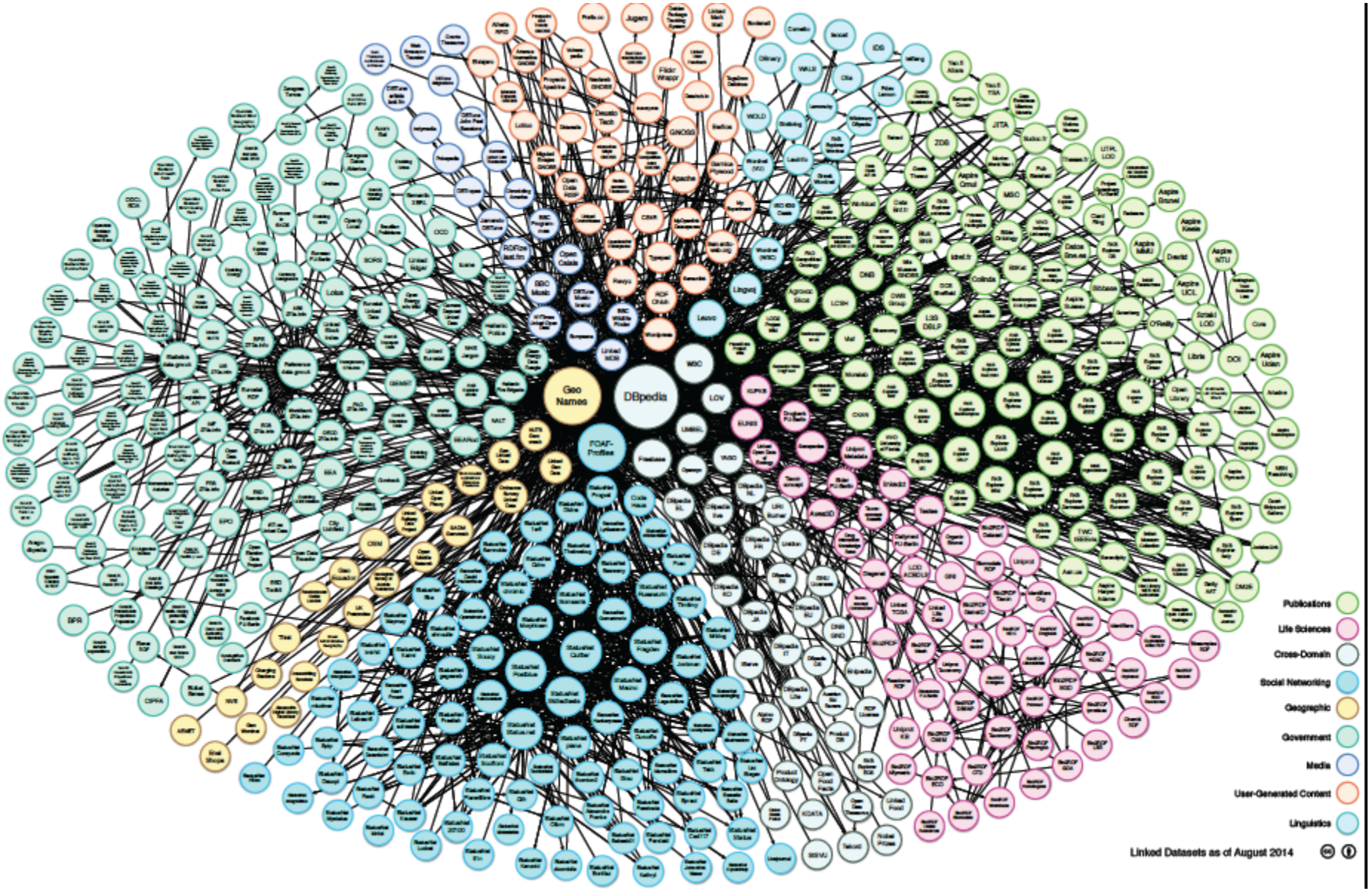
E1. DBpedia

Linking Open Data cloud diagram, by Richard Cyganiak and Anja Jentzsch. http://lod-cloud.net/

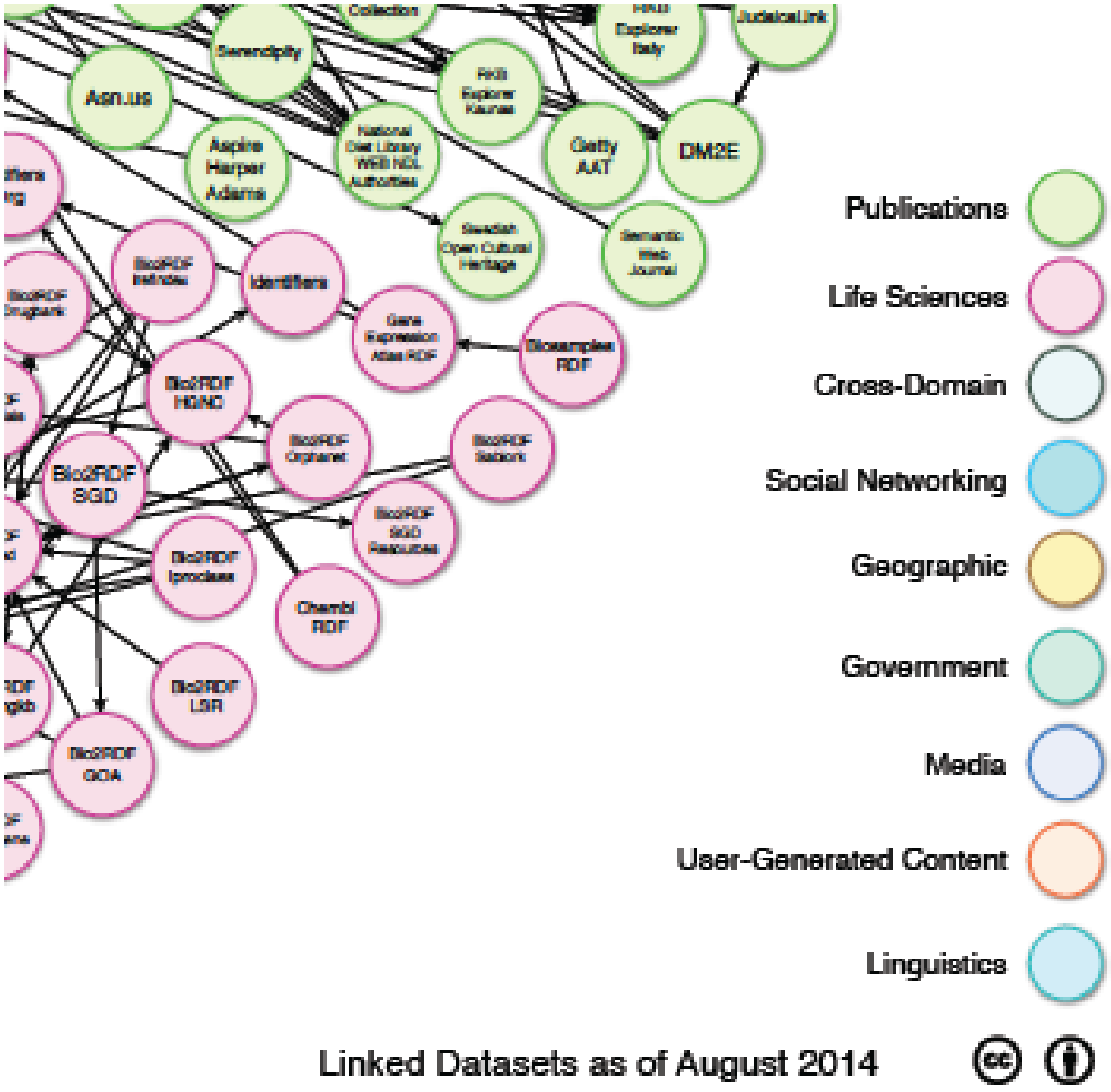


Linking Open Data cloud diagram, by Richard Cyganiak and Anja Jentzsch. http://lod-cloud.net/

Example 1: Open Source Intelligence LODC-DBpedia)



Linking Open Data cloud diagram 2014, by Max Schmachtenberg, Christian Bizer, Anja Jentzsch and Richard Cyganiak. http://lod-cloud.net/



Linked Datasets as of August 2014

lod-cloud_colored.pdf - Adobe Acrobat Pro
Archivo Edición Ver Ventana Ayuda
Crear

Table 1: Number of datasets in each category and growth compared to 2011.

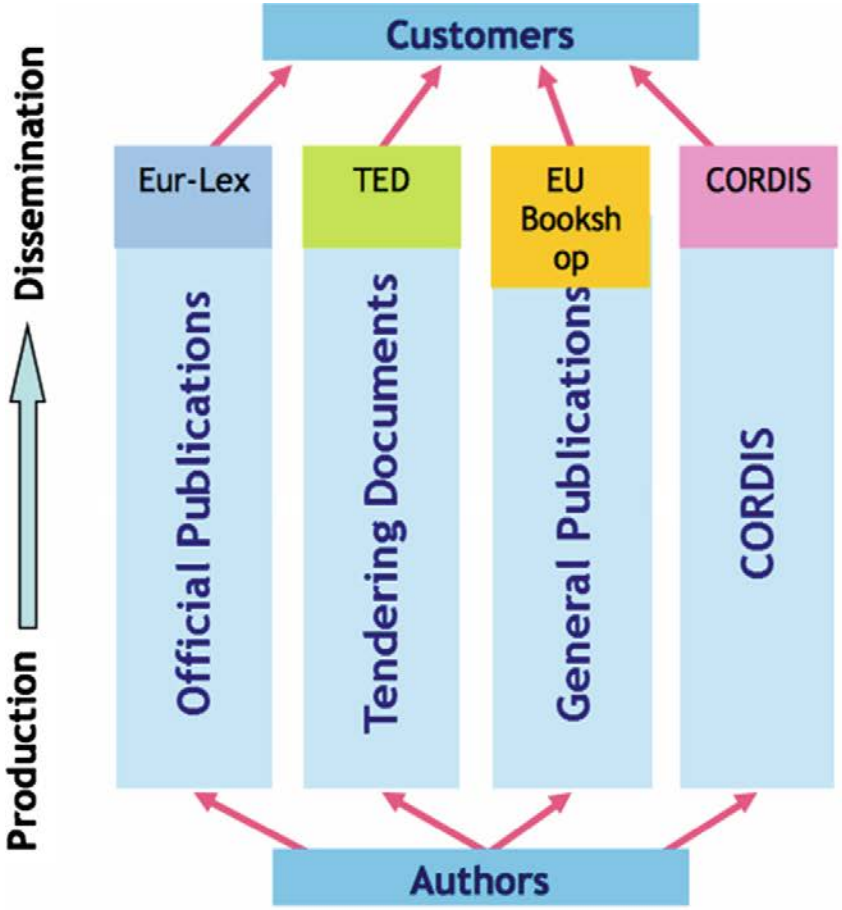
Category	Datasets 2014	Percentage	Datasets 2011	Growth
Media	24 (-2)	2%	25	-4%
Government	199 (-16)	18%	49	306%
Publications	138 (-42)	13%	87	59%
Geographic	27 (-6)	2%	31	-13%
Life Sciences	85 (-2)	8%	41	107%
Cross-domain	47 (-6)	4%	41	15%
User-generated Content	51 (-3)	5%	20	155%
Social Networking	520 (-0)	48%	-	-
Total	1091 (-77)		294	271%

Adoption of the Linked Data Best Practices in Different Topical Domains

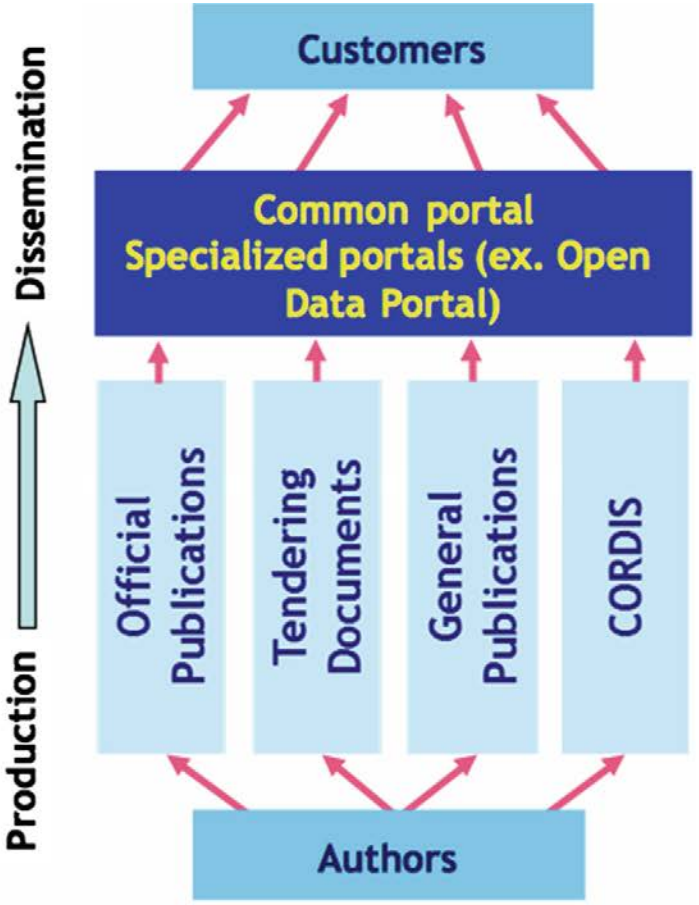
Max Schmachtenberg, Christian Bizer, and Heiko Paulheim

University of Mannheim
Research Group Data and Web Science
{max,chris,heiko}@informatik.uni-mannheim.de

E2. CELLAR (2015)

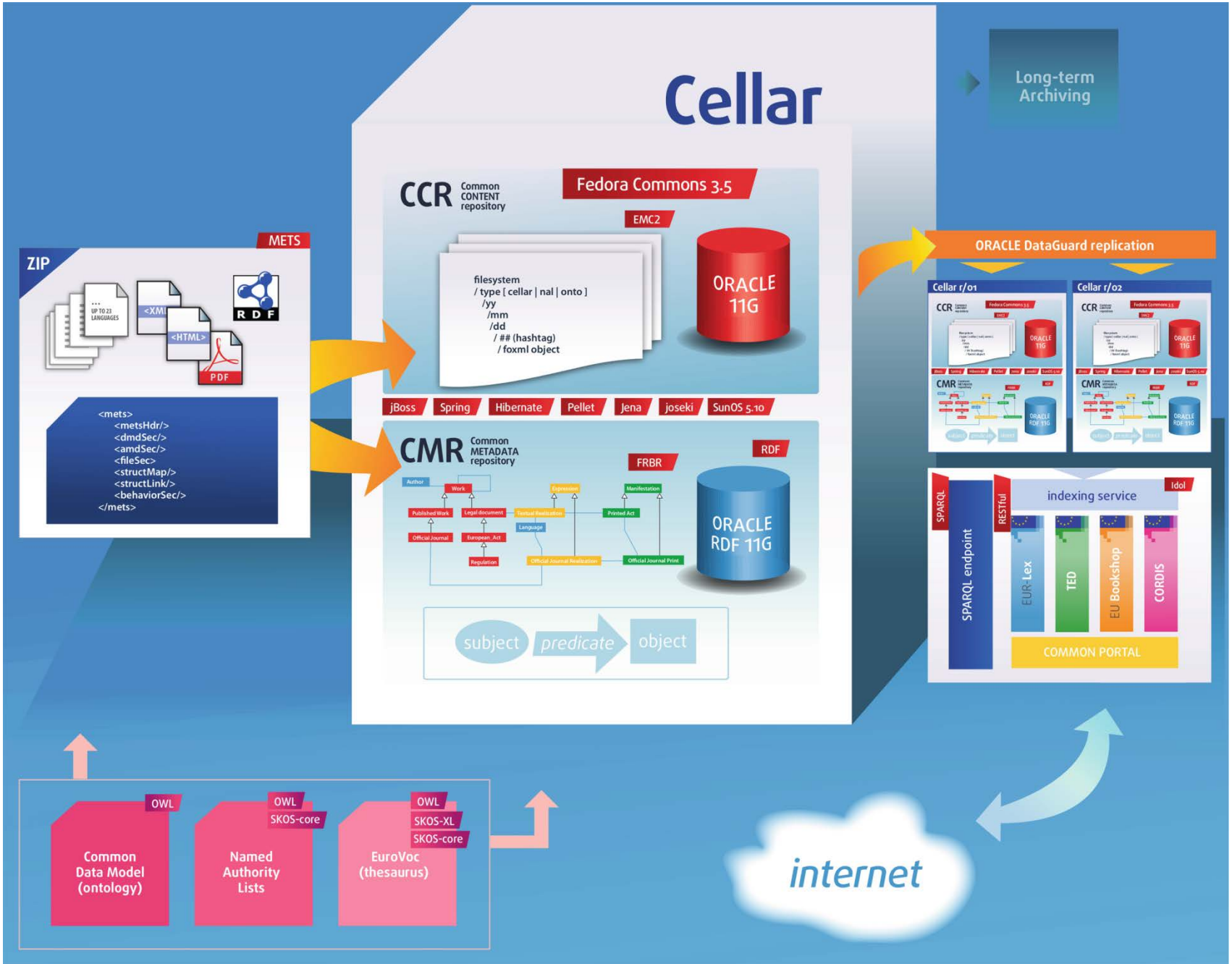


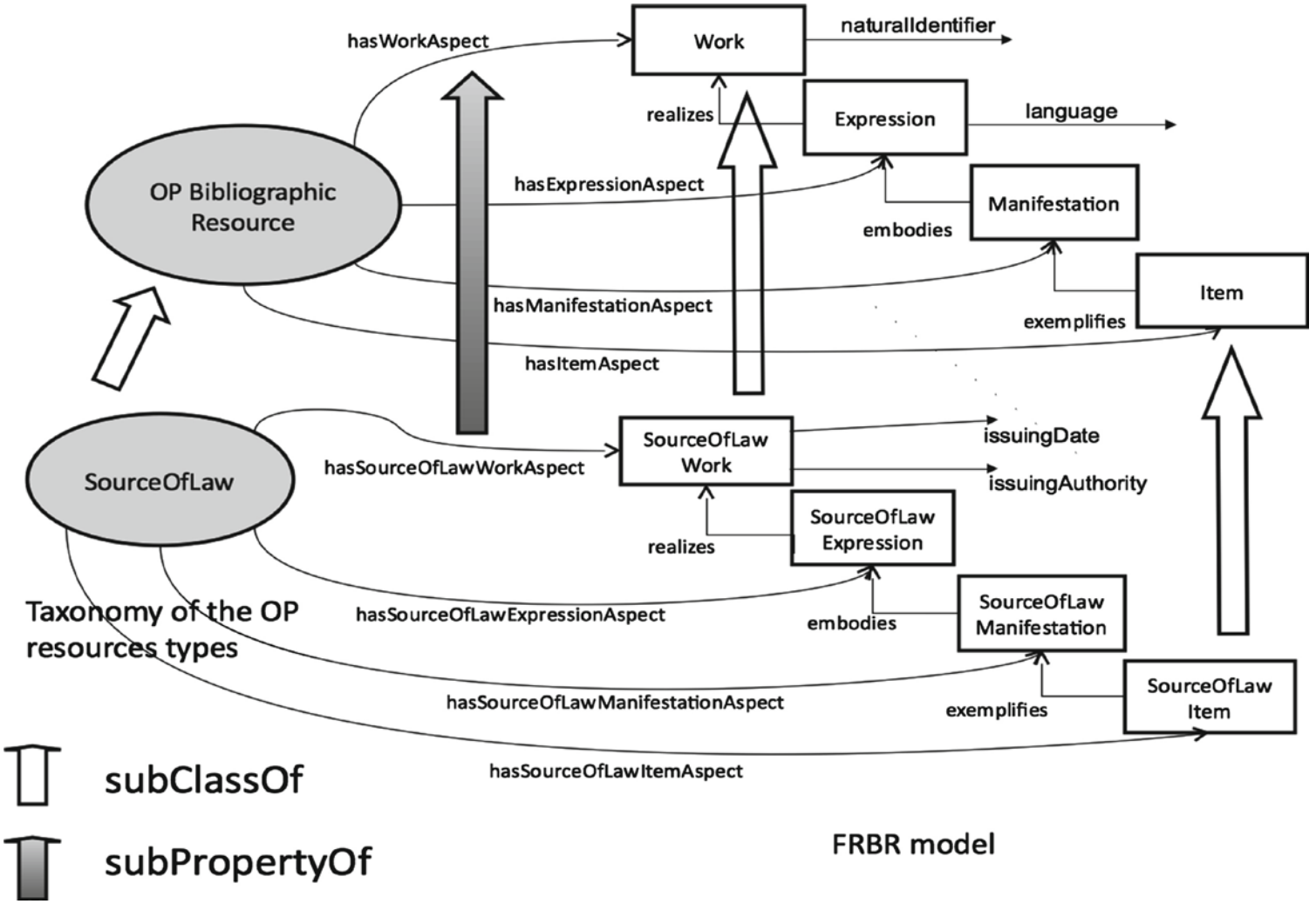
Old Architecture



New Architecture

Datos vinculados CELLAR (EurLEX, Francesconi, Sanmartín, 2015)

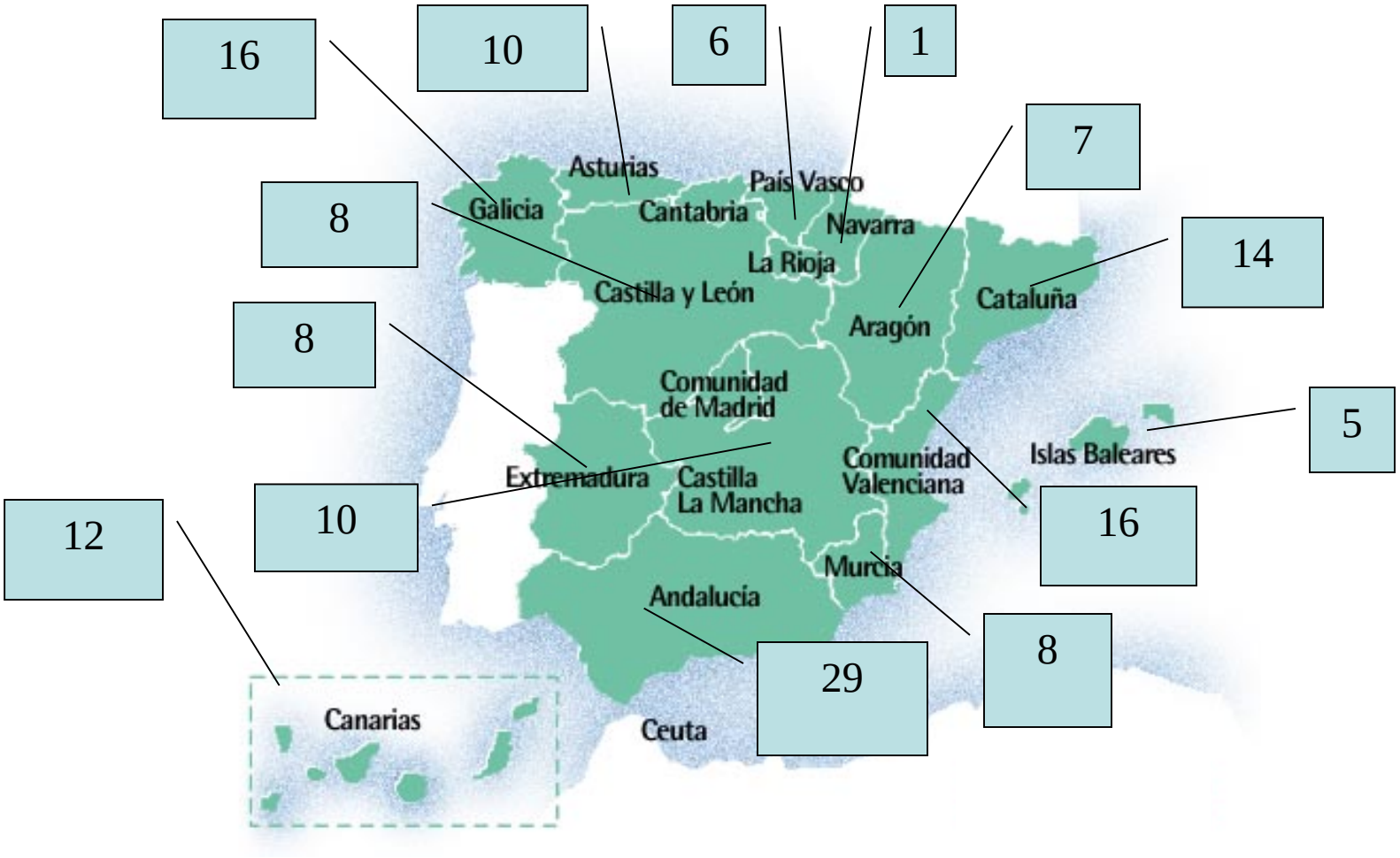

Cellar
Long-term Archiving
ZIP
METS
UP TO 23 LANGUAGES
<XML>
<HTML>
PDF
RDF
<mets>
<metsHdr/>
<dmdSec/>
<amdSec/>
<fileSec>
<structMap/>
<structLink/>
<behaviorSec/>
</mets>
CCR Common CONTENT repository
Fedora Commons 3.5
EMC2
filesystem
/ type [cellar | nal | onto]
/yy
/mm
/dd
/ ## (hashtag)
/ foxml object
ORACLE 11G
jBoss
Spring
Hibernate
Pellet
Jena
joseki
SunOS 5.10
CMR Common METADATA repository
FRBR
RDF
Author
Work
Published Work
Legal document
Official Journal
European_Act
Regulation
Expression
Textual Realization
Language
Manifestation
Printed Act
Official Journal Realization
Official Journal Print
ORACLE RDF 11G
subject
predicate
object
ORACLE DataGuard replication
Cellar r/o1
Cellar r/o2
SPARQL
SPARQL endpoint
RESTful
indexing service
Idol
EUR-Lex
TED
EU Bookshop
CORDIS
COMMON PORTAL
OWL
Common Data Model (ontology)
OWL
SKOS-core
Named Authority Lists
OWL
SKOS-XL
SKOS-core
EuroVoc (thesaurus)
internet



Esquema para la ontología de metadatos de CELLAR (2015)

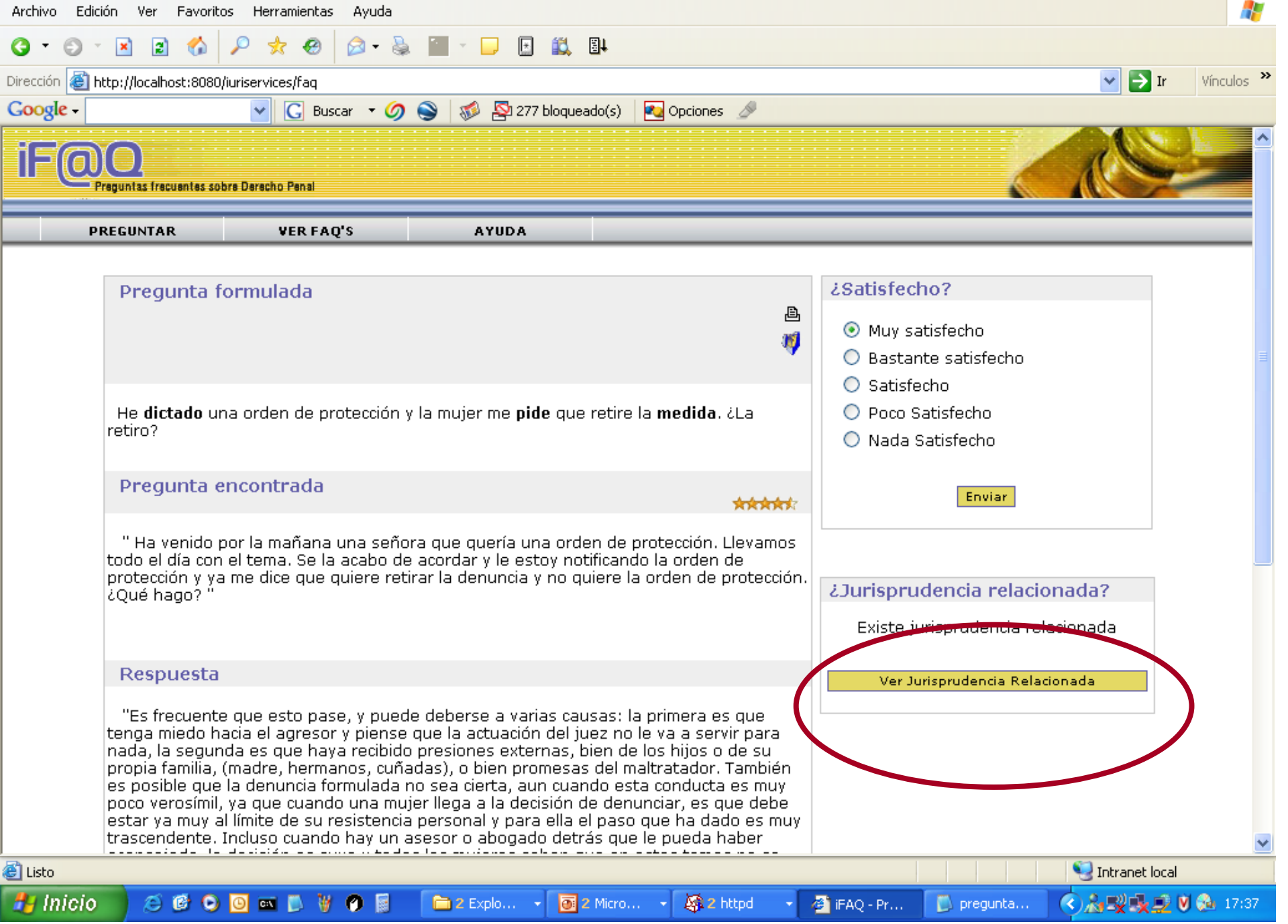
Cognitive walkthrough

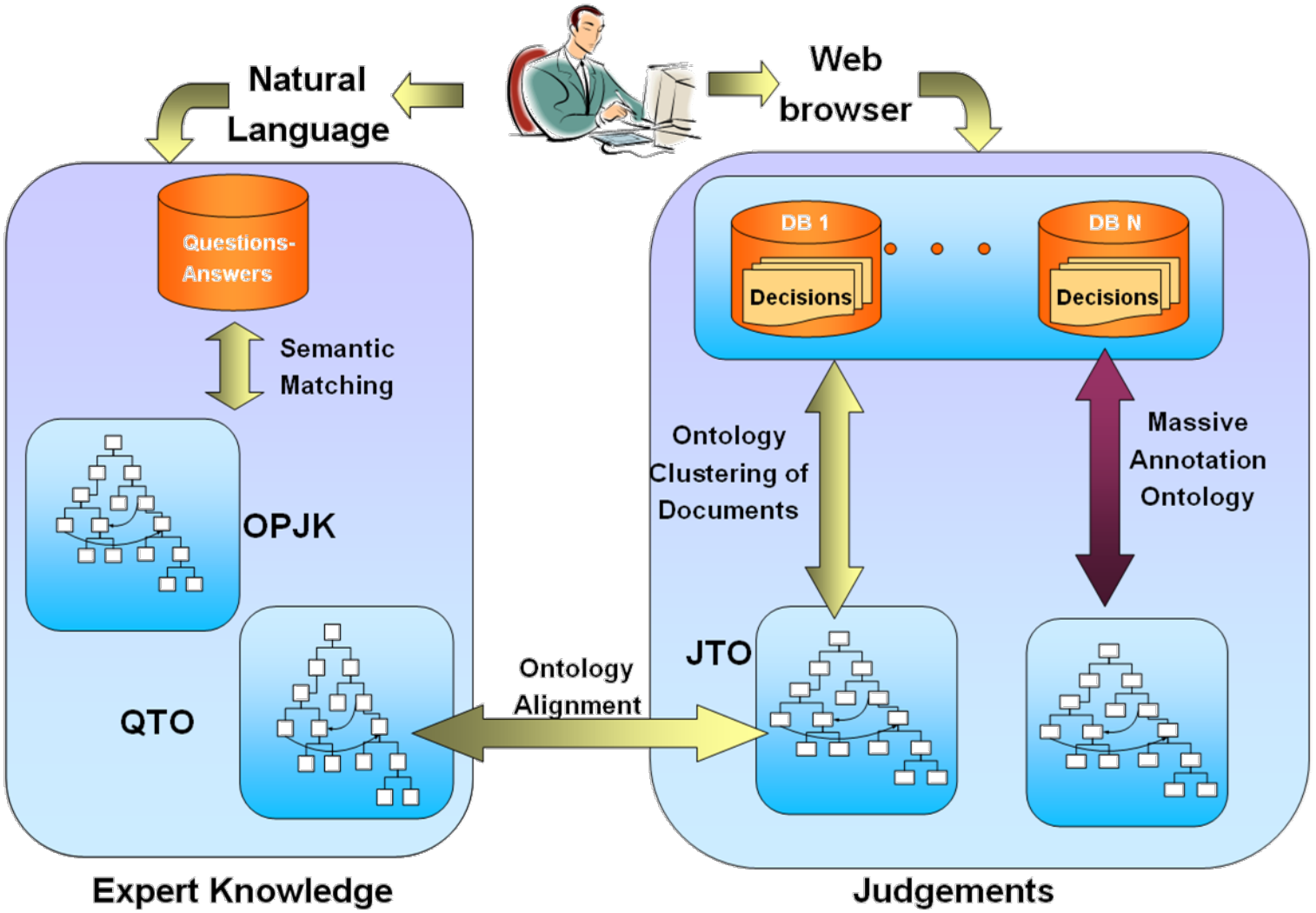
Distribución territorial de la etnografía



14 de las 17 Comunidades Autónomas

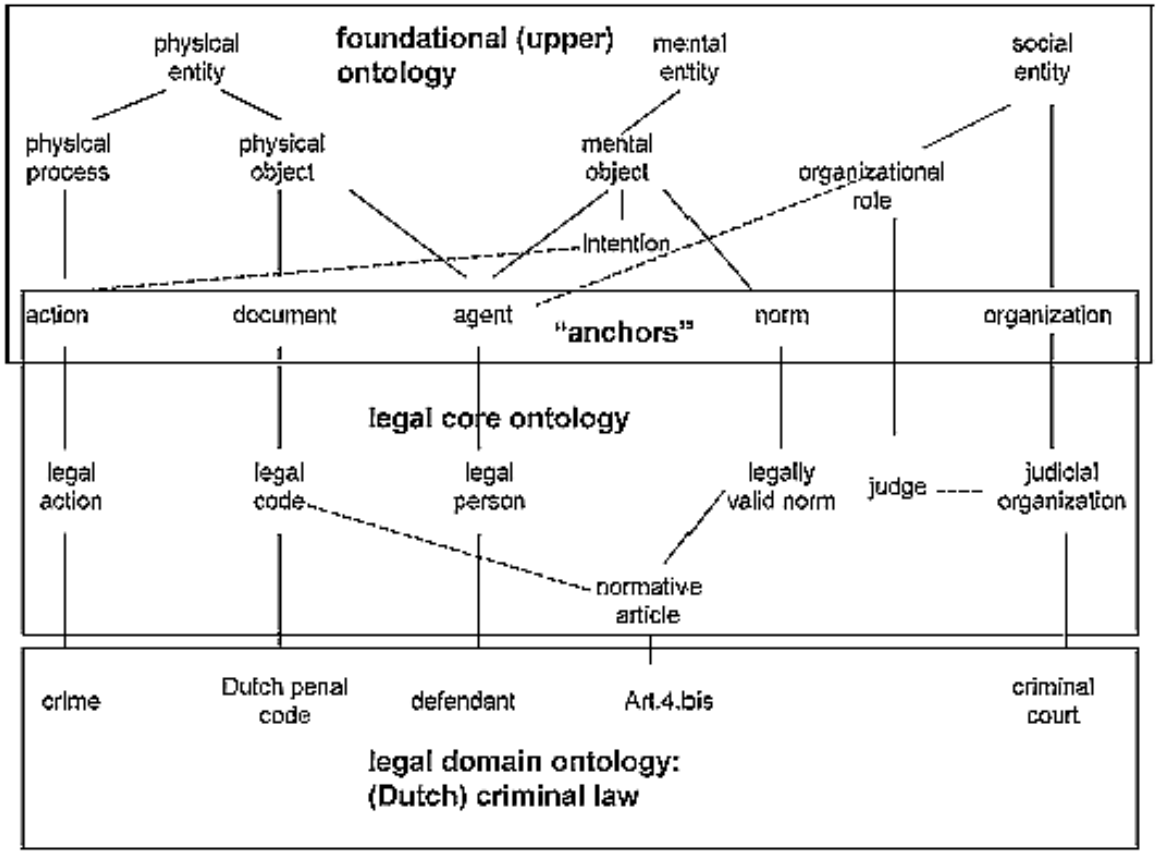
Villaviciosa (Asturias)


Archivo Edición Ver Favoritos Herramientas Ayuda
Dirección http://localhost:8080/iuriservices/faq
Ir
Vínculos
Google
Buscar
277 bloqueado(s)
Opciones
iF@Q
Preguntas frecuentes sobre Derecho Penal
PREGUNTAR
VER FAQ'S
AYUDA
Pregunta formulada
He dictado una orden de protección y la mujer me pide que retire la medida. ¿La retiro?
Pregunta encontrada
" Ha venido por la mañana una señora que quería una orden de protección. Llevamos todo el día con el tema. Se la acabo de acordar y le estoy notificando la orden de protección y ya me dice que quiere retirar la denuncia y no quiere la orden de protección. ¿Qué hago? "
Respuesta
"Es frecuente que esto pase, y puede deberse a varias causas: la primera es que tenga miedo hacia el agresor y piense que la actuación del juez no le va a servir para nada, la segunda es que haya recibido presiones externas, bien de los hijos o de su propia familia, (madre, hermanos, cuñadas), o bien promesas del maltratador. También es posible que la denuncia formulada no sea cierta, aun cuando esta conducta es muy poco verosímil, ya que cuando una mujer llega a la decisión de denunciar, es que debe estar ya muy al límite de su resistencia personal y para ella el paso que ha dado es muy trascendente. Incluso cuando hay un asesor o abogado detrás que le pueda haber
¿Satisfecho?
Muy satisfecho
Bastante satisfecho
Satisfecho
Poco Satisfecho
Nada Satisfecho
Enviar
¿Jurisprudencia relacionada?
Existe jurisprudencia relacionada
Ver Jurisprudencia Relacionada
Listo
Intranet local
Inicio
2 Explo...
2 Micro...
2 httpd
iFAQ - Pr...
pregunta...
17:37



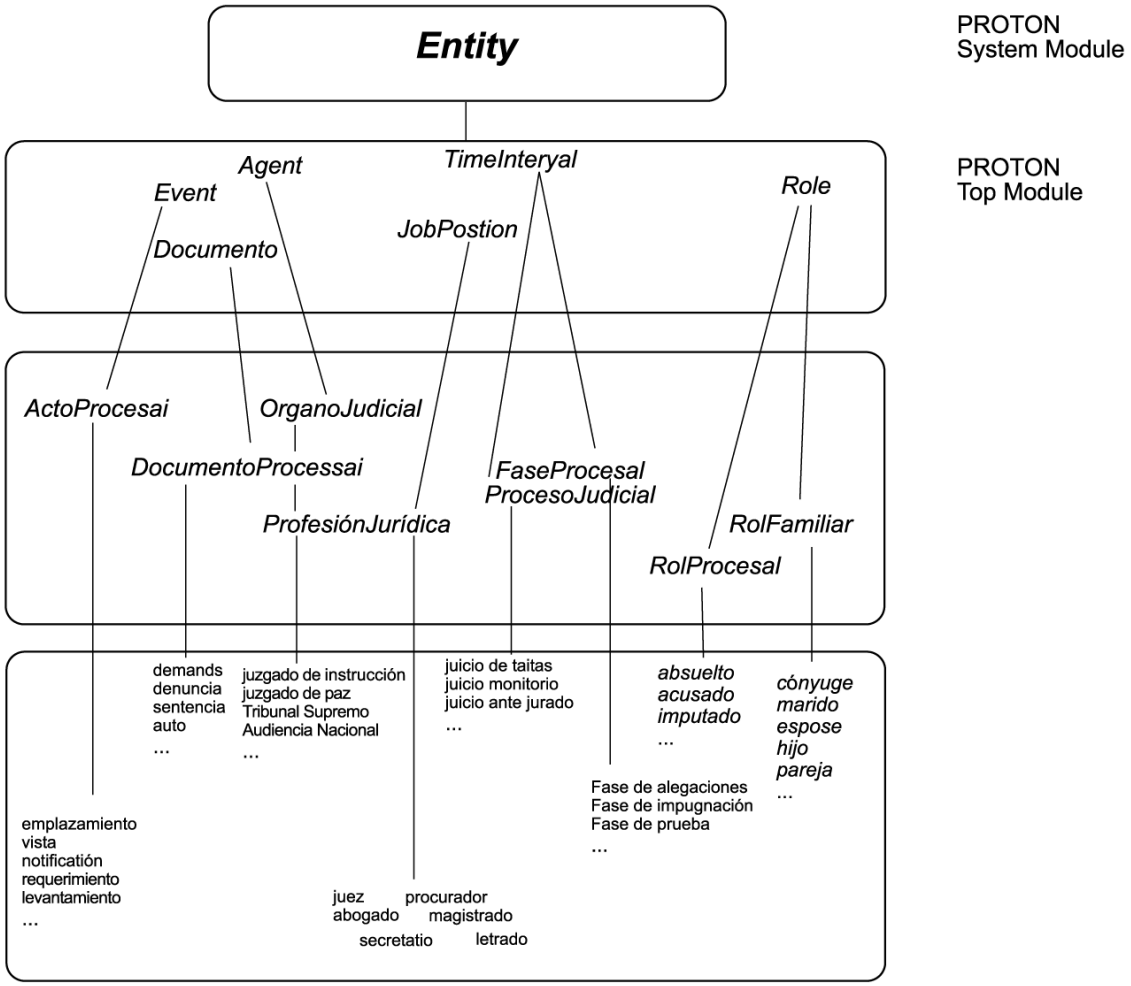
Arquitectura de Iuriservice: SEKT 2006

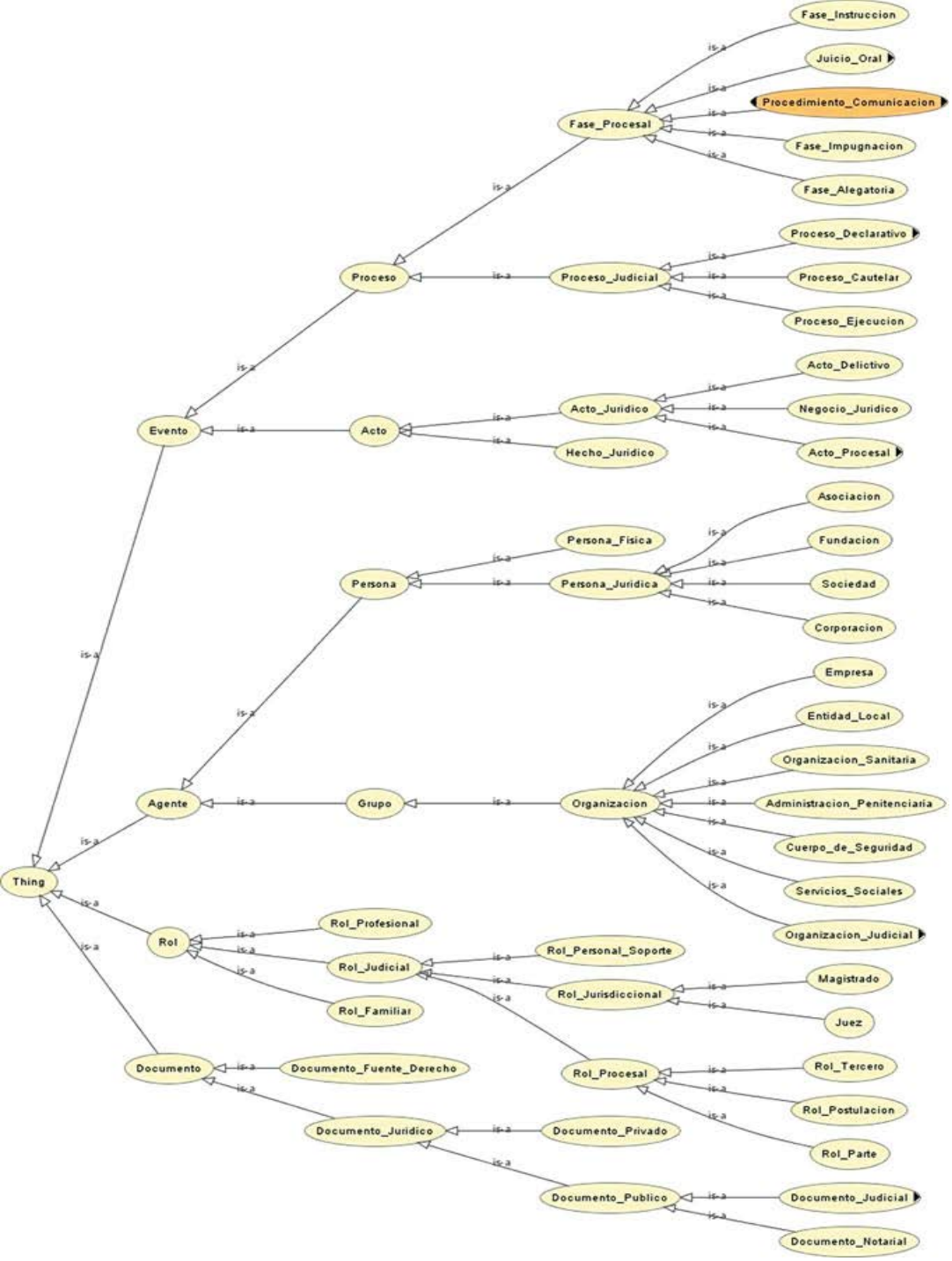
Niveles de ontología jurídica (FOL)



Source: Breuker *et al.*; in A. Gangemi, J. Breuker (2002: 29).

Iuriservice (2005)



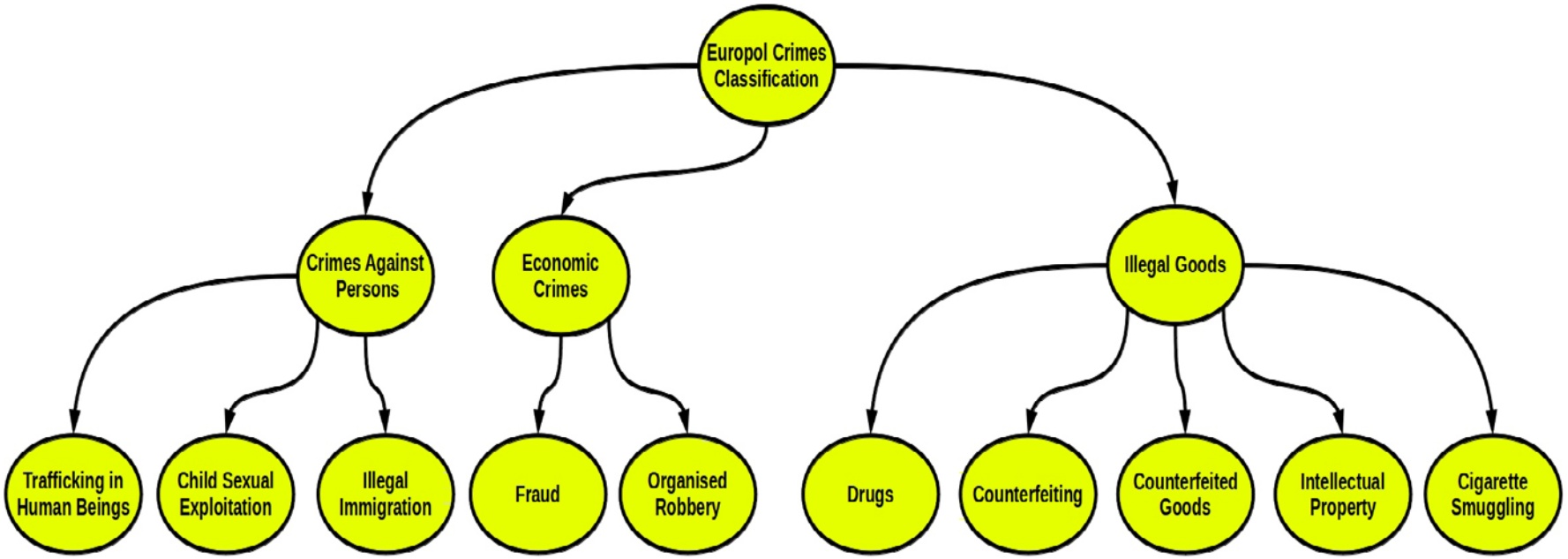


OPJK
Casellas
(2011)

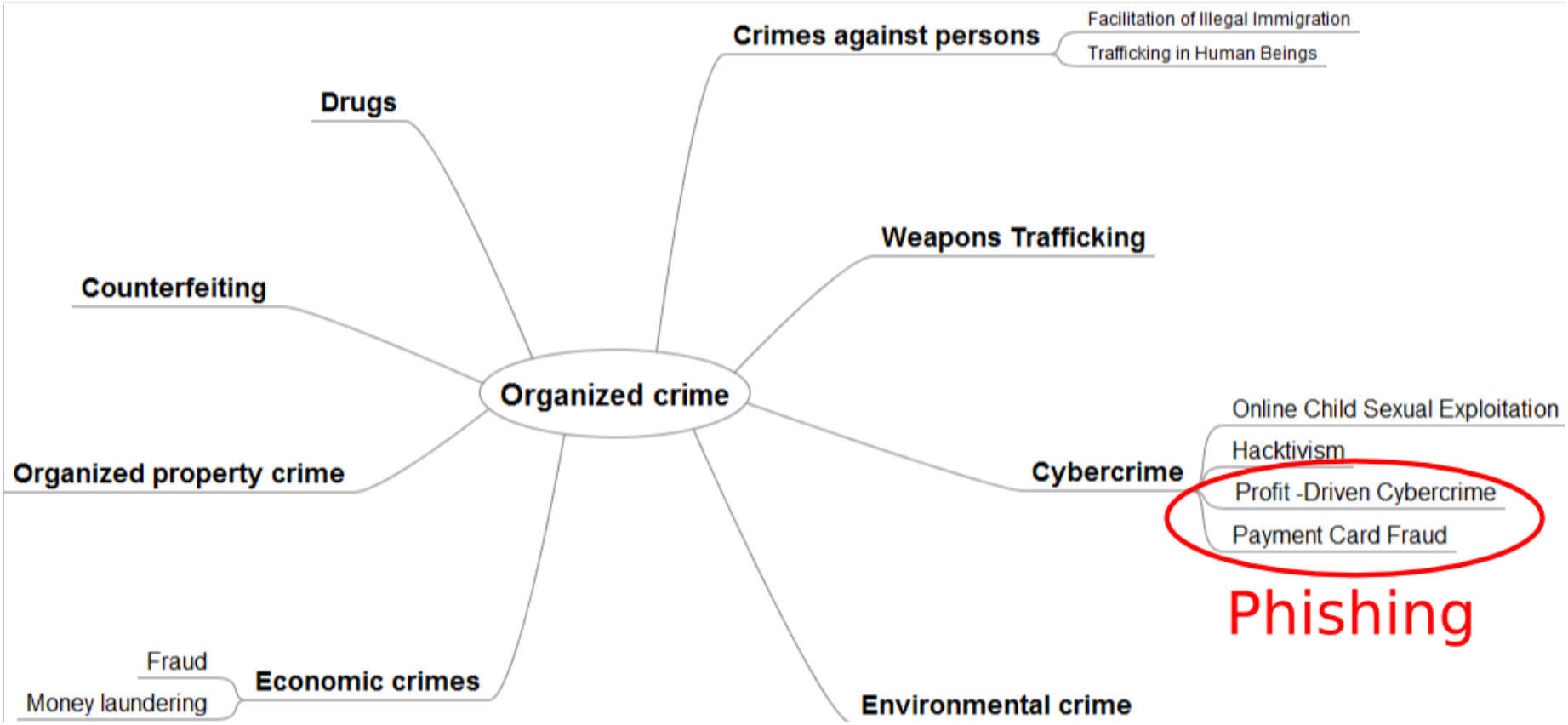
El Proyecto CAPER

E4. CAPER (2013)

Crime Taxonomy (from Europol)



Crimen organizado



Source: Europol SOCTA 2013

Objetivos de CAPER

- a) Implementar un marco para conectar datos demúltiples fuentes mediante múltiples técnicas de visualización
- b) Importación de datos para mejorar las prestaciones policiales contra el crimen organizado y organizar la cooperación policial europea
- c) Ayudar al descubriemiento de patrones y documentación para incrementar la capacidad de detección de delitos.
- d) Cuatro componentes del sistema: (i) Cultivo y adquisición de datos, (ii) Análisis (procesamiento de contenido), (iii) Almacenaje y consulta de información, y (iv) visualización avanzada de datos.

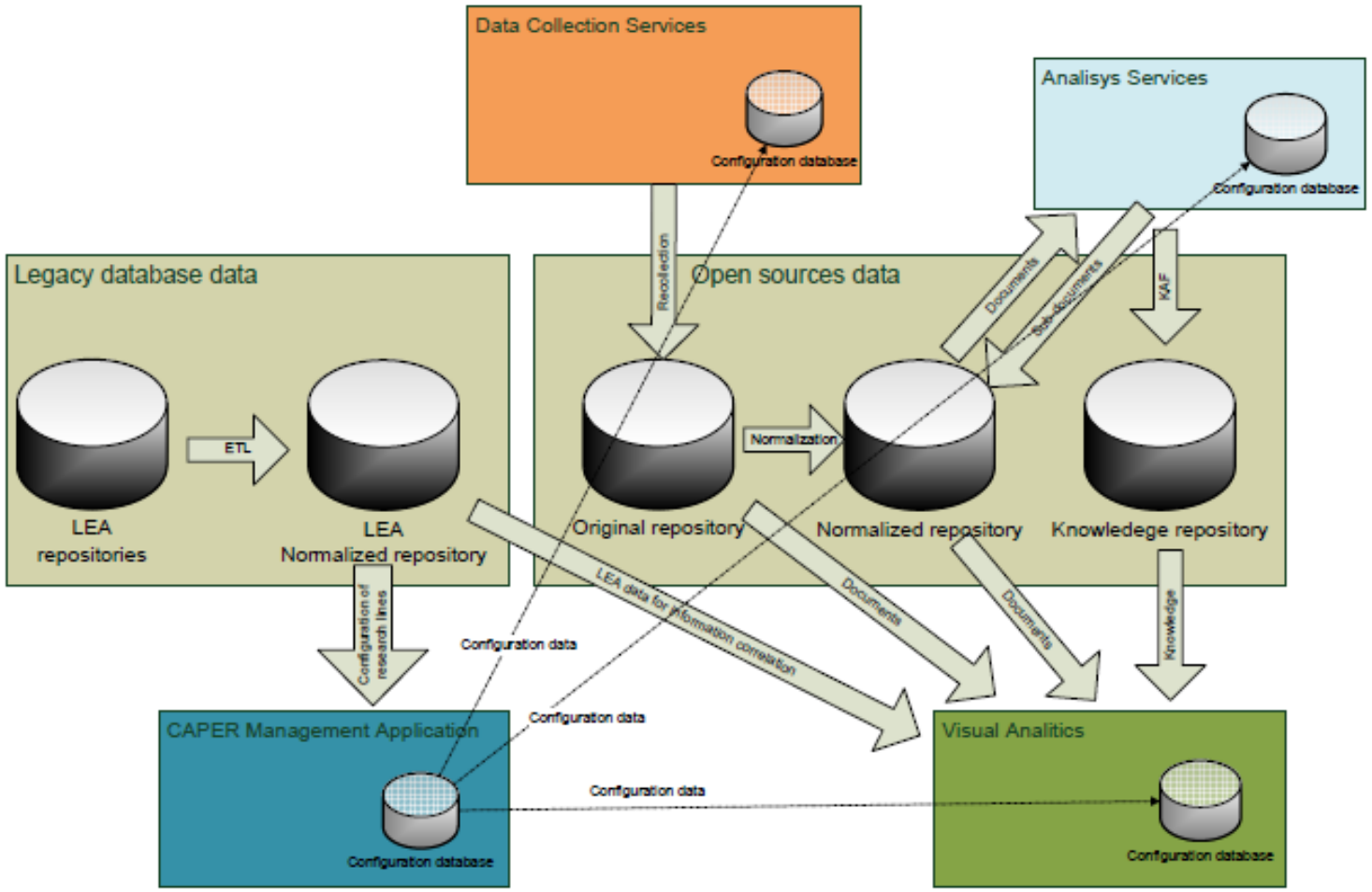
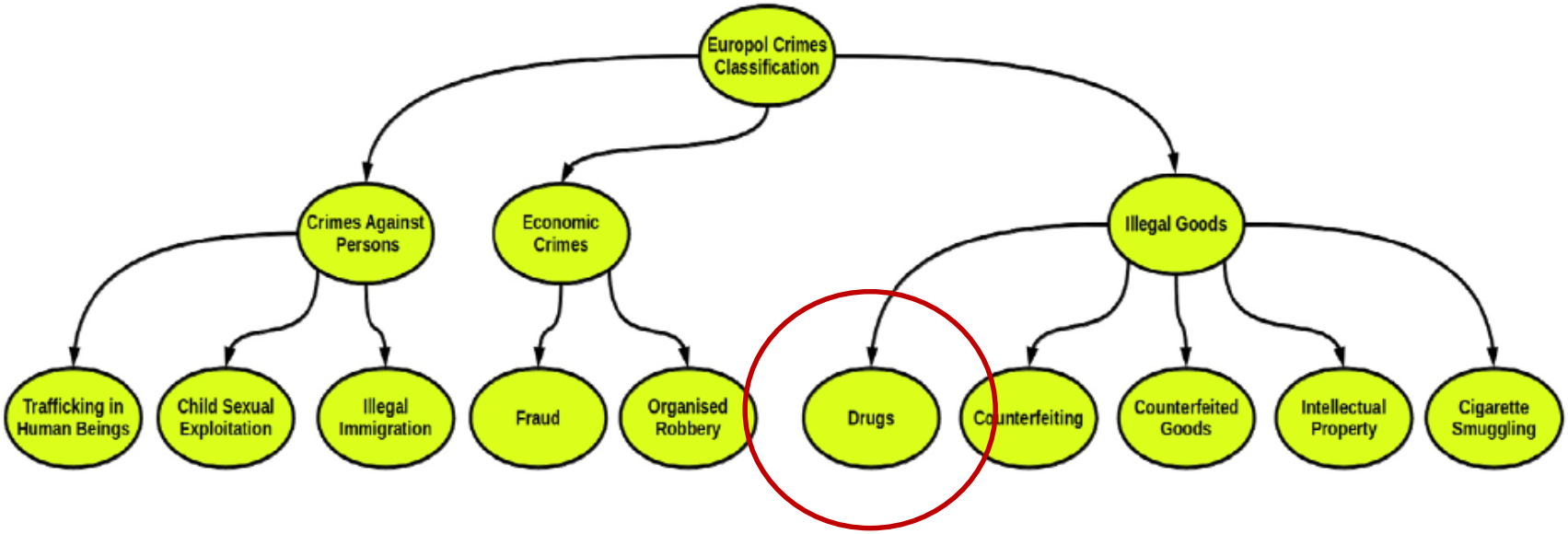
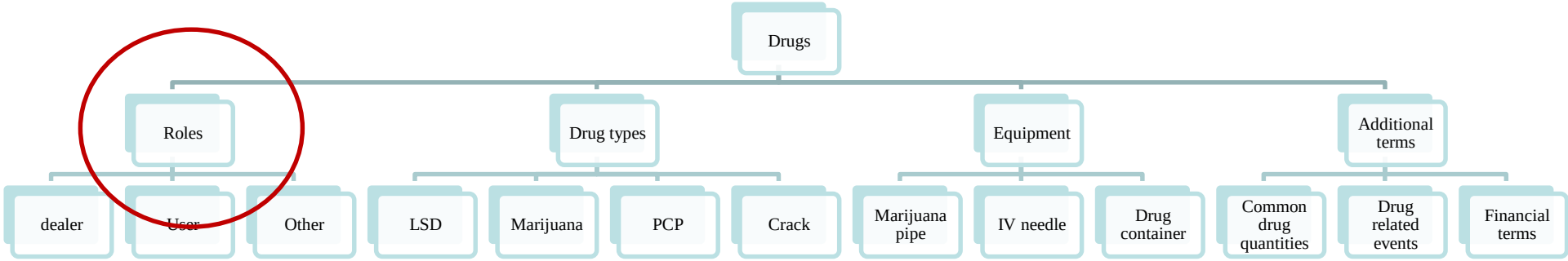


Figure 12 - CAPER databases overview

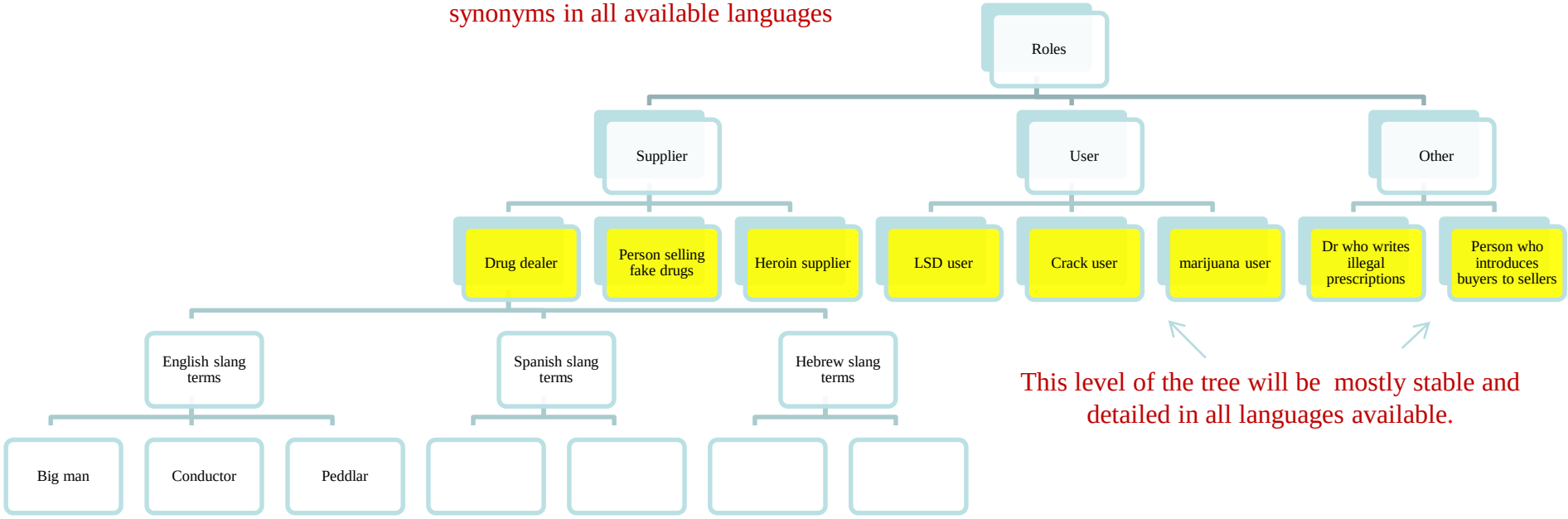
Cómo puede regularse el flujo de información?

Linguistic Ontologies: Gila Molcho, Teknion, Haifa



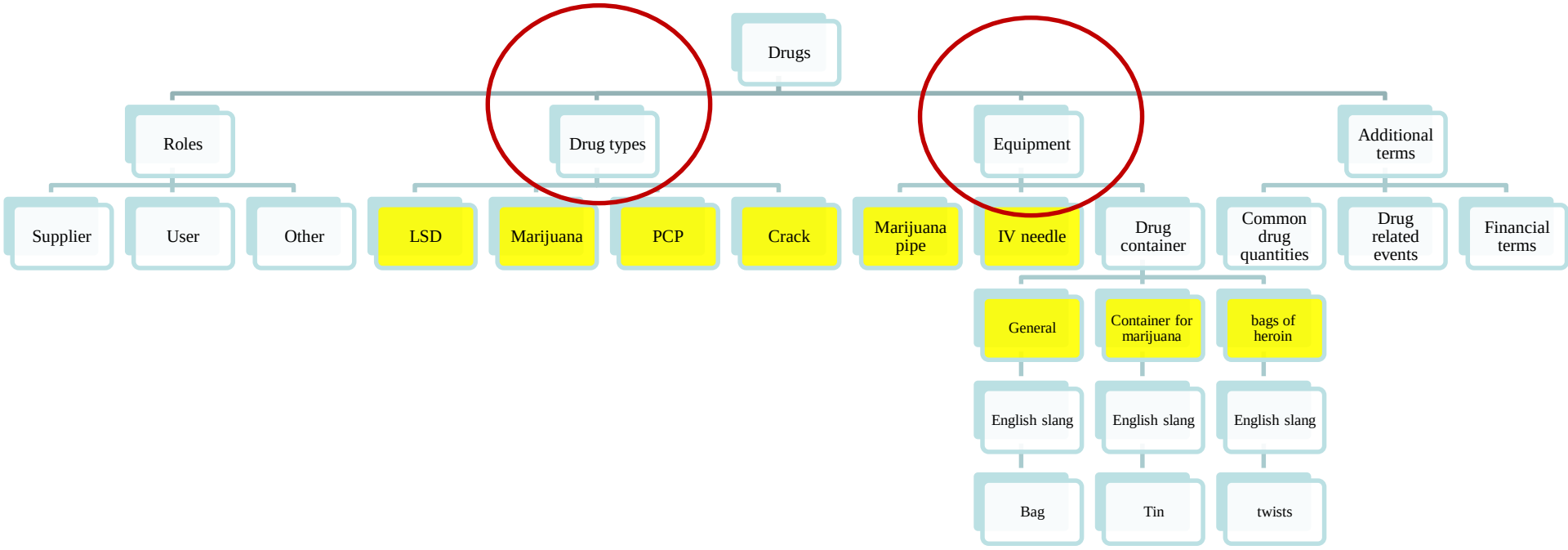

Drugs
Roles
dealer
User
Other
Drug types
LSD
Marijuana
PCP
Crack
Equipment
Marijuana pipe
IV needle
Drug container
Additional terms
Common drug quantities
Drug related events
Financial terms

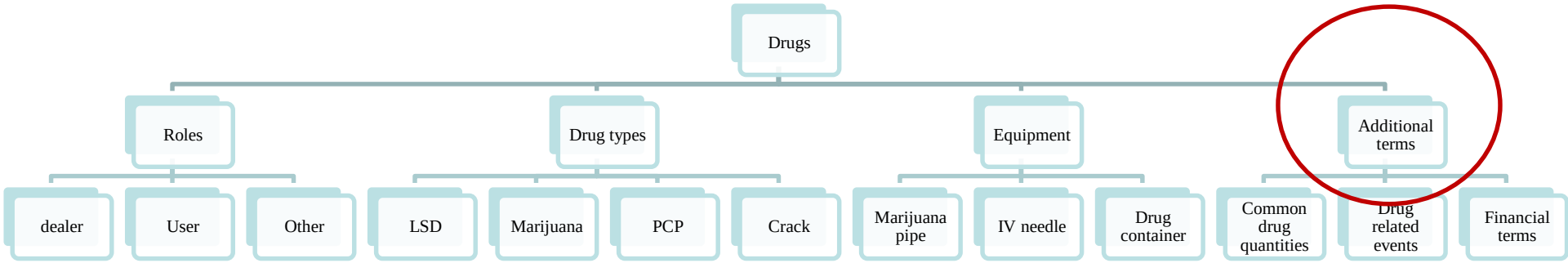
The basic tree will be multilingual (by attribute) and mostly stable
Each term will have both translations and synonyms in all available languages

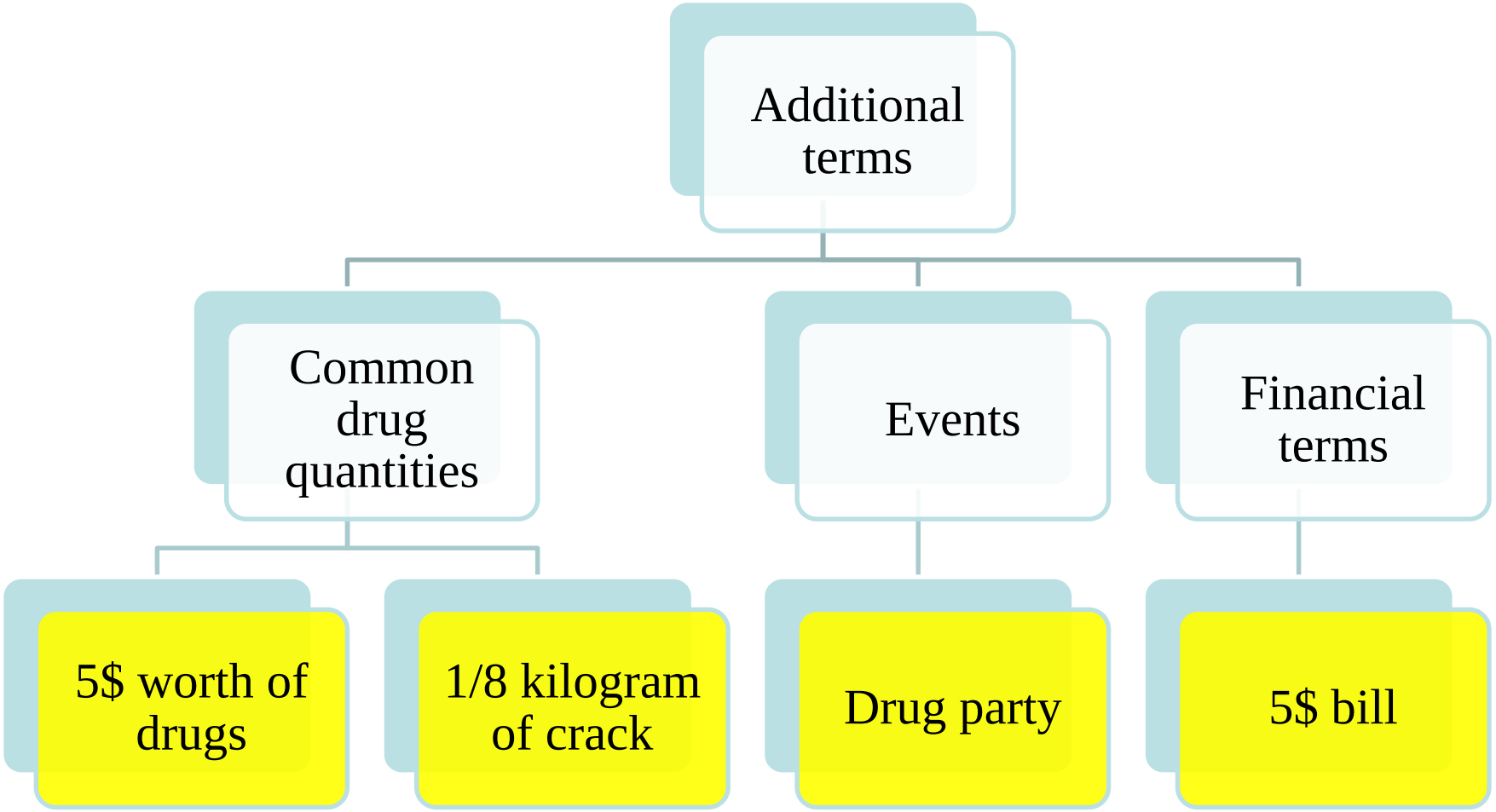


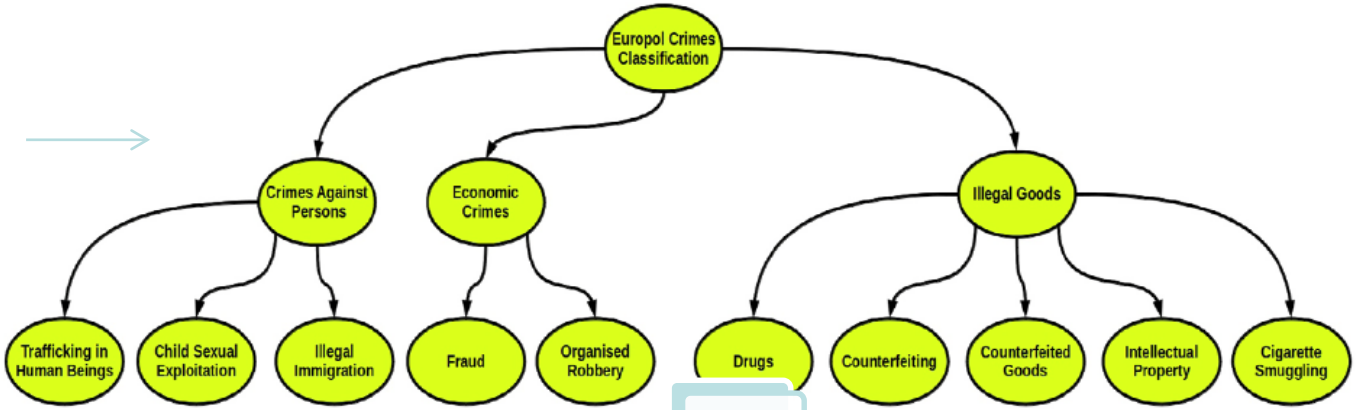
This level of the tree will be mostly stable and detailed in all languages available.

This leaf level will be dynamic and updatable

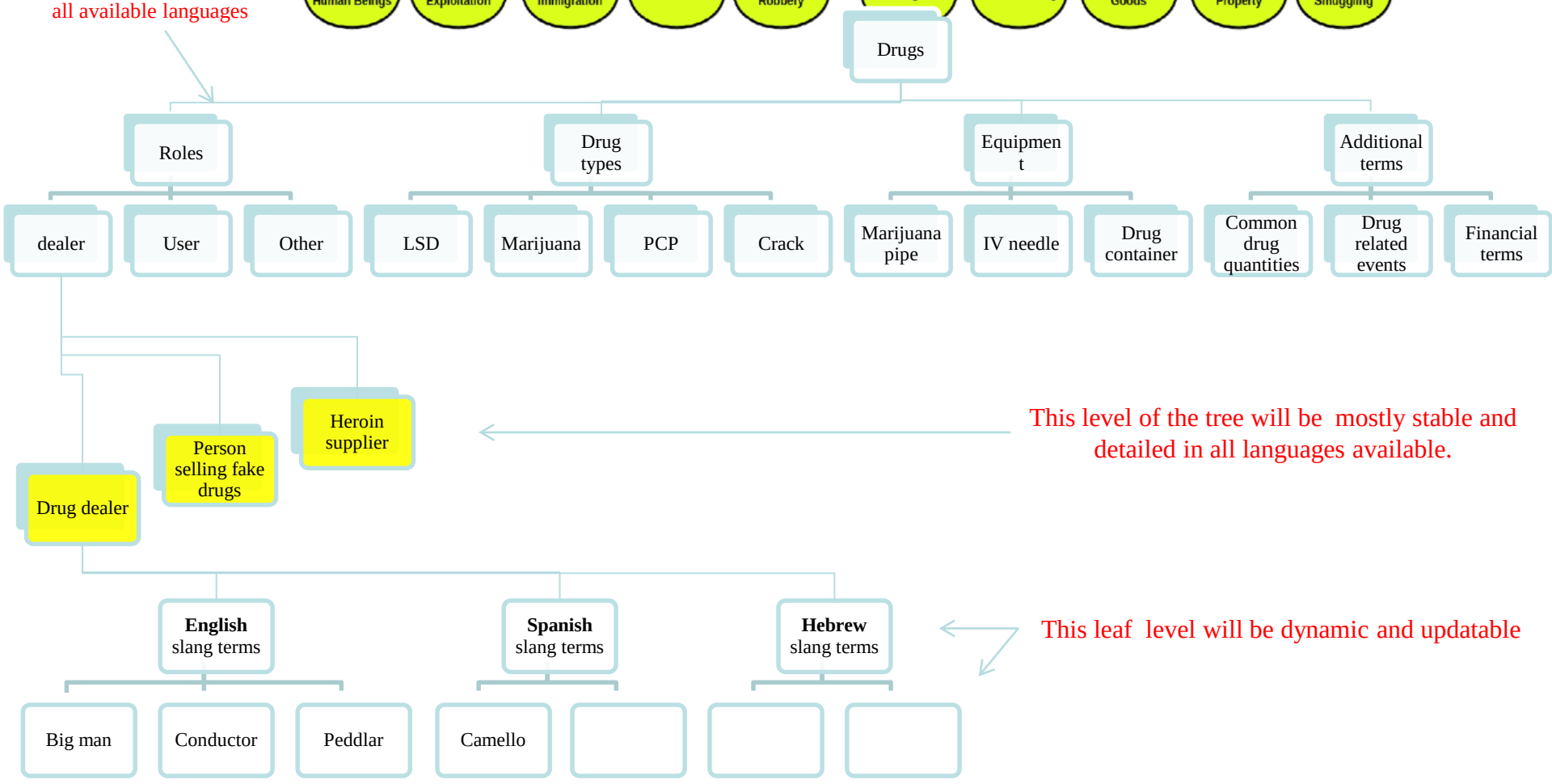

Drugs
Roles
Supplier
User
Other
Drug types
LSD
Marijuana
PCP
Crack
Equipment
Marijuana pipe
IV needle
Drug container
General
English slang
Bag
Container for marijuana
English slang
Tin
bags of heroin
English slang
twists
Additional terms
Common drug quantities
Drug related events
Financial terms


Drugs
Roles
Drug types
Equipment
Additional terms
dealer
User
Other
LSD
Marijuana
PCP
Crack
Marijuana pipe
IV needle
Drug container
Common drug quantities
Drug related events
Financial terms


Additional terms
Common drug quantities
Events
Financial terms
5$ worth of drugs
1/8 kilogram of crack
Drug party
5$ bill



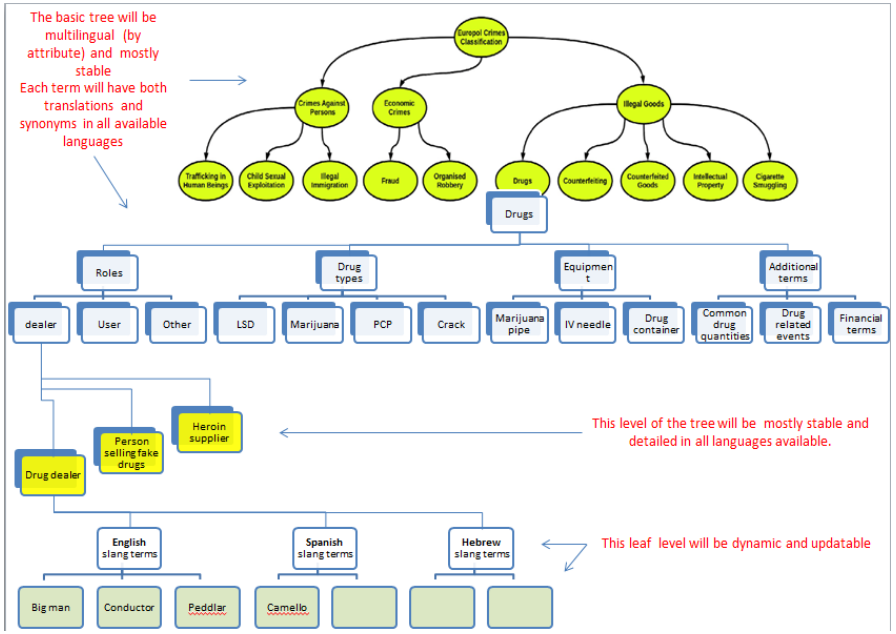
The basic tree will be multilingual (by attribute) and mostly stable
Each term will have both translations and synonyms in all available languages



This level of the tree will be mostly stable and detailed in all languages available.

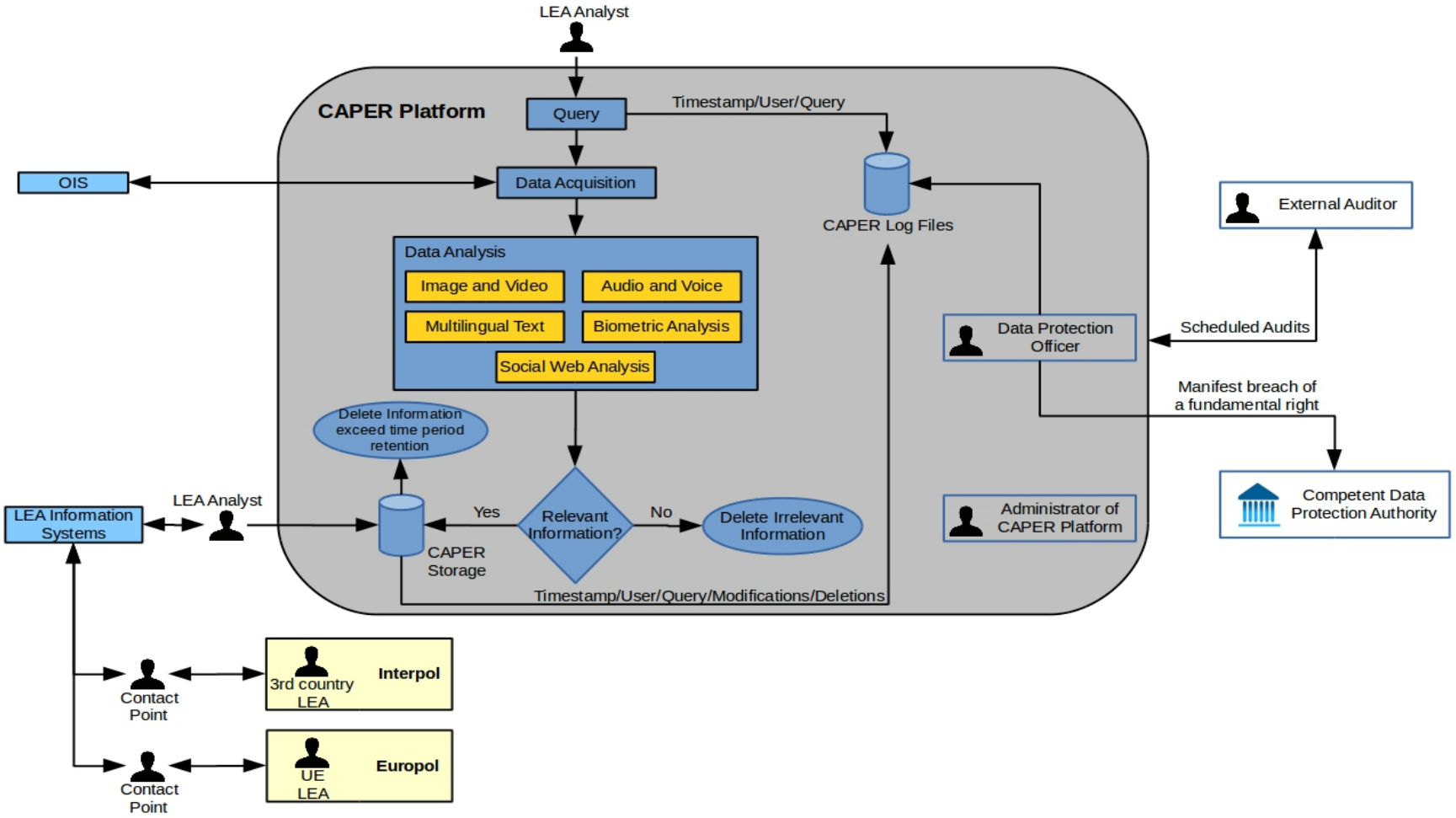
This leaf level will be dynamic and updatable

High level ontology. Based on Europol crime Classification.
Multilingual, quite stable. Synonyms and equivalencies in different languages.
Requests to LEAs: please validate classification and provide translations, synonyms and equivalencies, etc.

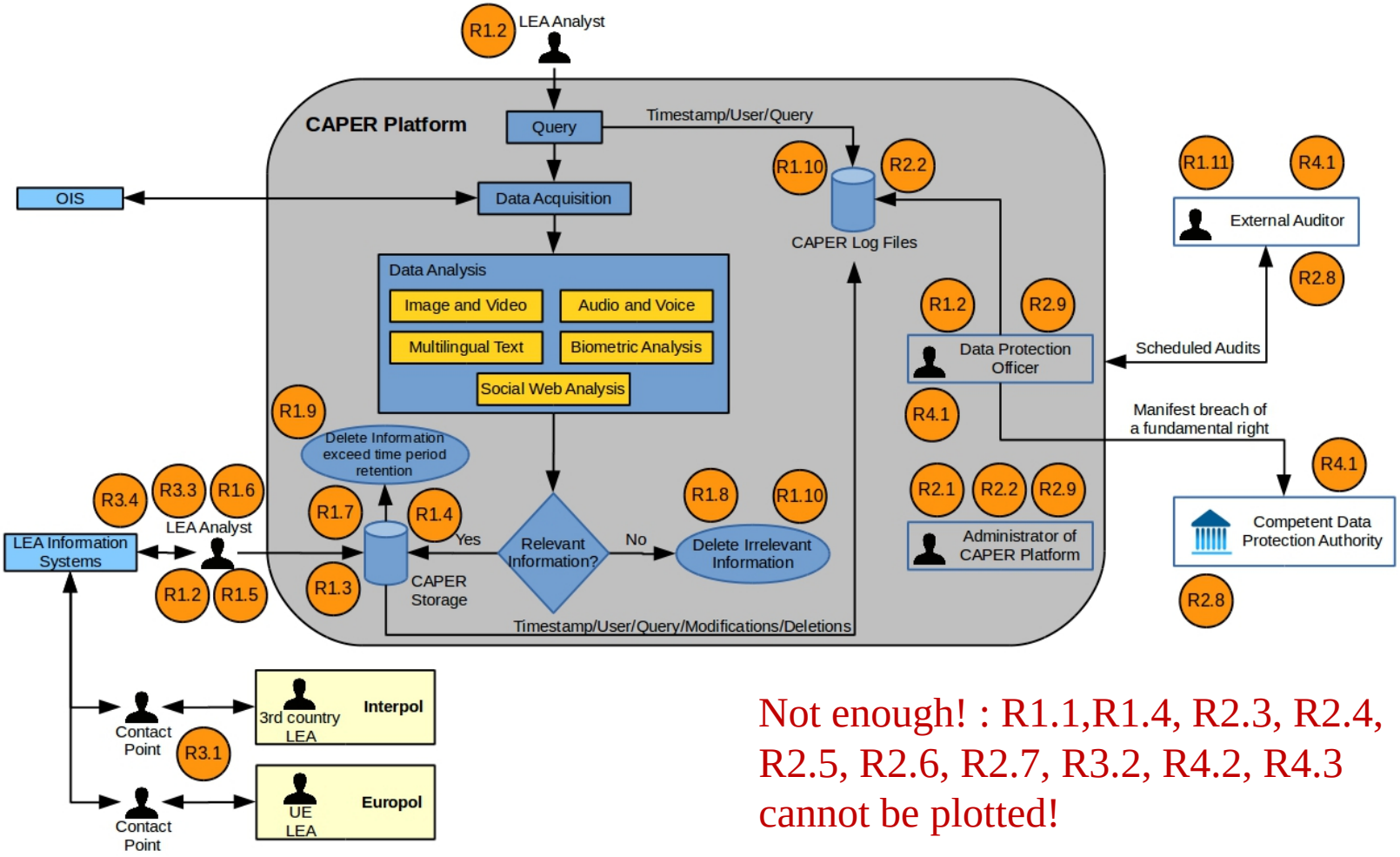


Specific use case (Drugs). To be implemented and embedded into CAPER platform (CMA and text analysis modules).
Multilingual, dynamic and updatable. Synonyms and equivalencies in different languages.
Requests to LEAs: please validate classification and provide translations, synonyms and equivalencies, etc.

CAPER Architecture flow



CAPER Architecture Flow and Rules



Not enough! : R1.1,R1.4, R2.3, R2.4, R2.5, R2.6, R2.7, R3.2, R4.2, R4.3 cannot be plotted!

CAPER Rules to regulate LEA's behaviour

I Data Collection and Storage	R1.1 Every LEA should perform a specific Privacy Impact Assessment (PIA) according to the general framework offered by the CAPER Regulatory Model (CRM).
	R1.4 No automated classification of suspects, victims and witnesses can be inferred from CAPER results.
II Data Management	R.2.3 Access to CAPER database should be granted for the purpose of prevention, detection or investigation of organized crime.
	R.2.4 Any other request of access for other purposes should be rejected.
	R.2.5 Non-authorised LEA and intelligence services or administrative bodies of authorized LEA should not have access to CAPER data.
	R.2.6 The use of system integrity tools should enable detection and reporting of changes applied on servers. In case of such an event the system should be able to notify specific users such as the creator of the query which results have been modified.
	R.2.7 Regular audits of the CAPER system should be performed by the external supervisor. The competent authority should be informed of the results, if necessary, according to national legislation, including the plans for enforcing recommendations.
III. Data Reuse and Transfer	R3.2 No automated classification of suspects, victims and witnesses can be inferred from CAPER results.
IV Right of Data Access	R.4.2 The reasons to deny access should be clear and defined. Access can be denied when the access may jeopardise the fulfilment of the LEA tasks, or the rights and freedoms of third parties.
	R.4.2 The alleged reasons to deny access should be open to external supervision. The external supervisory authority should have free access to documents justifying the refusal. A short time-span of three months to give an answer to a previous request of access should be implemented.

Efectos jurídicos!

- Ninguna clasificación de sospechosos, víctimas o testigos puede ser inferida automáticamente
- Consecuencia: la prueba no puede estar basada sólo en resultados de CAPER

- **..... Es mejor construir el CRM como una institución auto-regulada (con controles internos y externos)**

I. Data Collection and Storage

1. Every LEA should perform a specific Privacy Impact Assessment (PIA) according to the general framework offered by the CAPER Regulatory Model (CRM).

2. Data collected and stored by CAPER must only be used for fighting organized crime.

3. The storage of the CAPER data should be implemented in a separate repository. No contact with ordinary criminal data bases should be allowed.

4. No automated classification of suspects, victims and witnesses can be inferred from CAPER results.

5. Caper does not label individuals or groups as suspects, victims and witnesses. This labelling is performed by a human analyst. Lately, an information management process should determine how the data is transferred to the LEAs Information Systems.

6. No automatic decision should substitute the police analysis by human experts. Time retention periods should be linked with the relevancy of the data, “no reason for storing irrelevant data or data that has become irrelevant” should be the rule. Not relevant/needed data in any investigation should be erased. There should be an automated tool detecting the end of the retention period and informing the competent LEA or controller so that they can take action if the data is still relevant /needed.

7. Regular audits of the CAPER system should be performed by the external supervisor. The competent authority should be informed of the results, if necessary according to national legislation, including the plans for enforcing recommendations.

8. The CAPER data management system deletes all the results when the search is already finished. All queries and results should be kept in a log file available for the control by the internal and external CAPER data supervisors.

Legal Effects!

- No classification of suspects, victims and witnesses can be automatically inferred.
- Consequence: evidence in Court cannot be based only on CAPER results

- **..... It is better to build CRM as a self-regulatory institution (with internal / external controls)**

PRINCIPLES OF FAIR INFORMATION PRACTICES (FIPs)

1. *Openness and transparency*	There should be no secret record keeping. This includes both the publication of the existence of such collections, as well as their contents.
2. *Individual participation*	The subject of a record should be able to see and correct the record.
3. *Collection limitation*	Data collection should be proportional and not excessive compared to the purpose of the collection.
4. *Data quality*	Data should be relevant to the purposes for which they are collected and should be kept up to date.
5. *Use limitation*	Data should only be used for their specific purpose by authorized personnel.
6. *Reasonable security*	Adequate security safeguards should be put in place, according to the sensitivity of the data collected.
7. *Accountability*	Record keepers must be accountable for compliance with the other principles.

FIPs. Source: Langheinrich (2001): Alan F. Westin (1967)

Privacy by Design Foundational Principles [Cameron-Cavoukian]	Fair Information Practice Principle (GPS) [Cavoukian]	Extended Principles [Cavoukian]	Semantic Web LOD Governemnt [Berners-Lee]	LII Principles [Greenleaf-Bruce]	ODR Principles [Zeleznikow-Bellucci]	Crowdsourcing Principles [Bott-Young]	Crisis Mapping Principles [Poblet-Meier]
1. Proactive not reactive; Preventative not Remedia		Established methods to **recognize** poor privacy designs, to **anticipate** poor privacy practices and outcomes, and to correct the negative impacts	Proactive modeling: XML, RDF, SPARQL, OWL	Technological investment	Willingness to enter into a negotiation, and be fair	Universal Participation: collaborative governance	Proactive participation, conflict prevention and crisis management
2. Privacy as the Default Setting	3. Purpose Specification 4. Collection Limitation, Data Mini-mization 5. Use, Retention Disclosure Limitation	Privacy becomes the prevailing condition - without the data subject ever having to ask for it -no action required.	Access, Data, Storage, Metadata, Ontologies, Alarm Systems, Trust	Republication, Anonymization	Fairness-Enabling Discovery (Disclosure Limitation)	Trust: disclosure limitation	Harmless Digital neighborhood Causing no harm
3. Privacy Embedded into Design		Systemic program or methodology in place to ensure that privacy is thoroughly integrated into operations standard-based and validable).	Architecture, Data protection, Storage, Metadata, Enrichment, Core Ontologies, Domain Ontologies, Rules, Principles, Trust, Validation	Republication Reusing Authentication (Authoritative versions) Integrity	Fairness-Bargaining in the shadow of the law and the use of BATNAs	Trust: Empowering people	Implementing Digital neighborhood Causing no harm
4. Full Functionality Positive-Sum, Not Zero-Sum		Multifunctional solutions: legitimate non-privacy interests and objectives, early, desired functions articulated, agreed metrics applied.	Access, Data protection, Metadata, Core Ontologies, Domain Ontologies, Rules, Principles, Trust, Validation	Balanced interests (publisher/state/user)	Fairness-Enabling Discovery (Privacy Limitation)	Trust: aggregated interests and values; monitorization, metrics applied	Trust: aggregated interests and values; monitored processes; metrics applied
5. End-to-End Security, Full Lifecycle Protection	7. Security		Ontology sustainability, folksonomies	Integrity, Security, Maintenance	Secure environment	Integrity: secure environment and paerticipation	Volunteers' Security
6. Visibility, Transparency Keep It Open	2. Accoun-tability 8. Opennes 10. Com-pliance		Accountable information systems and decisions; Content value, tagging and semantic enrichment	Accountability, Distributed Authority of republished materials	Developing transparency	Trust: Transparency	Trust: Transparency
7. Respect for User Privacy Keep it User-Centric	1. Consent 6. Accuracy 9. Access		End user-centered systems, personalization, middle-out ontology approach	Consent , Integrity, Content and added value preservation	Accuracy	Aggregated value	Accuracy of the information

Comparaison of Regulatory Principles:

Privacy, SW LOD (W3), LII, ODR, Crowdsourcing, Crisis Mapping

Privacy by Design Foundational Principles [Cameron-Cavoukian]	Fair Information Practice Principle (GPS) [Cavoukian]	Extended Principles [Cavoukian]	Semantic Web LOD Governemnt [Berners-Lee]	LII Principles [Greenleaf-Bruce]	ODR Principles [Zeleznikow-Bellucci]	Crowdsourcing Principles [Bott-Young]	Crisis Mapping Principles [Poblet-Meier]
1. Proactive not reactive; Preventative not Remedia		Established methods to **recognize** poor privacy designs, to **anticipate** poor privacy practices and outcomes, and to correct the negative impacts	Proactive modeling: XML, RDF, SPARQL, OWL	Technological investment	Willingness to enter into a negotiation, and be fair	Universal Participation: collaborative governance	Proactive participation, conflict prevention and crisis management
Users as Individuals			**Data**	**Providers**	**Process**	**Users as People**	**Users as Reporting People**
2. Privacy as the Default Setting	3. Purpose Specification 4. Collection Limitation, Data Mini-mization 5. Use, Retention Disclosure Limitation	Privacy becomes the prevailing condition - without the data subject ever having to ask for it -no action required.	Access, Data, Storage, Metadata, Ontologies, Alarm Systems, Trust	Republication, Anonymization	Fairness-Enabling Discovery (Disclosure Limitation)	Trust: disclosure limitation	Harmless Digital neighborhood Causing no harm
3. Privacy Embedded into Design		Systemic program or methodology in place to ensure that privacy is thoroughly integrated into operations standard-based and validable).	Architecture, Data protection, Storage, Metadata, Enrichment, Core Ontologies, Domain Ontologies, Rules, Principles, Trust, Validation	Republication Reusing Authentication (Authoritative versions) Integrity	Fairness-Bargaining in the shadow of the law and the use of BATNAs	Trust: Empowering people	Implementing Digital neighborhood Causing no harm
4. Full Functionality Positive-Sum, Not Zero-Sum		Multifunctional solutions: legitimate non-privacy interests and objectives, early, desired functions articulated, agreed metrics applied.	Access, Data protection, Metadata, Core Ontologies, Domain Ontologies, Rules, Principles, Trust, Validation	Balanced interests (publisher/state/user)	Fairness-Enabling Discovery (Privacy Limitation)	Trust: aggregated interests and values; monitorization, metrics applied	Trust: aggregated interests and values; monitored processes; metrics applied
5. End-to-End Security, Full Lifecycle Protection	7. Security		Ontology sustainability, folksonomies	Integrity, Security, Maintenance	Secure environment	Integrity: secure environment and paerticipation	Volunteers' Security
6. Visibility, Transparency Keep It Open	2. Accoun-tability 8. Opennes 10. Com-pliance		Accountable information systems and decisions; Content value, tagging and semantic enrichment	Accountability, Distributed Authority of republished materials	Developing transparency	Trust: Transparency	Trust: Transparency
7. Respect for User Privacy Keep it User-Centric	1. Consent 6. Accuracy 9. Access		End user-centered systems, personalization, middle-out ontology approach	Consent , Integrity, Content and added value preservation	Accuracy	Aggregated value	Accuracy of the information

Privacy by Design Foundational Principles [Cameron-Cavoukian]	Fair Information Practice Principle (GPS) [Cavoukian]	Extended Principles [Cavoukian]	Semantic Web LOD Governemnt [Berners-Lee]	LII Principles [Greenleaf-Bruce]	ODR Principles [Zeleznikow-Bellucci]	Crowdsourcing Principles [Bott-Young]	Crisis Mapping Principles [Poblet-Meier]
1. Proactive not reactive; Preventative not Remedia		Established methods to **recognize** poor privacy designs, to **anticipate** poor privacy practices and outcomes, and to correct the negative impacts	Proactive modeling: XML, RDF, SPARQL, OWL	Technological investment	Willingness to enter into a negotiation, and be fair	Universal Participation: collaborative governance	Proactive participation, conflict prevention and crisis management
2. Privacy as the Default Setting	3. Purpose Specification 4. Collection Limitation, Data Mini-mization 5. Use, Retention Disclosure Limitation	Privacy becomes the prevailing condition - without the data subject ever having to ask for it -no action required.	Access, Data, Storage, Metadata, Ontologies, Alarm Systems, Trust	Republication, Anonymization	Fairness-Enabling Discovery (Disclosure Limitation)	Trust: disclosure limitation	Harmless Digital neighborhood Causing no harm
3. Privacy Embedded into Design		Systemic program or methodology in place to ensure that privacy is thoroughly integrated into operations standard-based and validable).	Architecture, Data protection, Storage, Metadata, Enrichment, Core Ontologies, Domain Ontologies, Rules, Principles, Trust Validation	Republication Reusing Authentication (Authoritative versions) Integrity	Fairness-Bargaining in the shadow of the law and the use of BATNAs	Trust: Empowering people	Implementing Digital neighborhood Causing no harm
4. Full Functionality Positive-Sum Not Zero-Sum		Multifunctional solutions: legitimate non-privacy interests and objectives, early, desired functions articulated, agreed metrics applied.	Access, Data protection, Metadata, Core Ontologies, Domain Ontologies, Rules, Principles, Trust Validation	Balanced interests (publisher/state/user)	Fairness-Enabling Discovery (Privacy Limitation)	Trust: aggregated interests and values; monitorization, metrics applied	Trust: aggregated interests and values; monitored processes; metrics applied
5. End-to-End Security, Full Lifecycle Protection	7. Security		Ontology sustainability, folksonomies	Integrity, Security, Maintenance	Secure environment	Integrity: secure environment and paerticipation	Volunteers' Security
6. Visibility, Transparency Keep It Open	2. Accoun-tability 8. Openness 10. Com-pliance		Accountable information systems and decisions, Content value, tagging and semantic enrichment	Accountability, Distributed Authority of republished materials	Developing transparency	Trust: Transparency	Trust: Transparency
7. Respect for User Privacy Keep it User Centric	1. Consent 6. Accuracy 9. Access		End user-centered systems, personalization, middle-out ontology approach	Consent , Integrity, Content and added value preservation	Accuracy	Aggregated value	Accuracy of the information

I PUBLIC CONSCIOUSNESS

II PUBLIC SPACE

III PUBLIC DOMAIN

IV PUBLIC GOVERNMENT

V PUBLIC NEIGHBORHOOD

Privacy by Design Foundational Principles [Cameron-Cavoukian]	Fair Information Practice Principle (GPS) [Cavoukian]	Extended Principles [Cavoukian]	Semantic Web LOD Governemnt [Berners-Lee]	LII Principles [Greenleaf-Bruce]	ODR Principles [Zeleznikow-Bellucci]	Crowdsourcing Principles [Bott-Young]	Crisis Mapping Principles [Poblet-Meier]
1. Proactive not reactive; Preventative not Remedia		Established methods to **recognize** poor privacy designs, to **anticipate** poor privacy practices and outcomes, and to correct the negative impacts	Proactive modeling: XML, RDF, SPARQL, OWL	Technological investment	Willingness to enter into a negotiation, and be fair	Universal Participation: collaborative governance	Proactive participation, conflict prevention and crisis management
2. Privacy as the Default Setting	3. Purpose Specification 4. Collection Limitation, Data Mini-mization 5. Use, Retention Disclosure Limitation	Privacy becomes the prevailing condition - without the data subject ever having to ask for it -no action required.	Access, Data, Storage, Metadata, Ontologies, Alarm Systems, Trust	Republication, Anonymization	Fairness-Enabling Discovery (Disclosure Limitation)	Trust: disclosure limitation	Harmless Digital neighborhood Causing no harm
3. Privacy Embedded into Design		Systemic program or methodology in place to ensure that privacy is thoroughly integrated into operations standard-based and validable). **Trust**	Architecture, Data protection, Storage, Metadata, Enrichment, Core Ontologies, Domain Ontologies, Rules, Principles, Trust Validation	Republication Reusing Authentication (Authoritative versions) Integrity **Republication**	Fairness-Bargaining in the shadow of the law and the use of BATNAs **Empowerment**	Trust: Empowering people	Implementing Digital neighborhood Causing no harm **Altruism**
4. Full Functionality Positive-Sum Not Zero-Sum		Multifunctional solutions: legitimate non-privacy interests and objectives, early, desired functions articulated, agreed metrics applied.	Access, Data protection, Metadata, Core Ontologies, Domain Ontologies, Rules, Principles, Trust Validation	Balanced interests (publisher/state/user)	Fairness-Enabling Discovery (Privacy Limitation) **Fairness**	Trust: aggregated interests and values; monitorization, metrics applied	Trust: aggregated interests and values; monitored processes; metrics applied
5. End-to-End Security, Full Lifecycle Protection	7. Security		Ontology sustainability, folksonomies	Integrity, Security, Maintenance	Secure environment	Integrity: secure environment and paerticipation	Volunteers' Security
6. Visibility, Transparency Keep It Open	2. Accoun-tability 8. Openness 10. Com-pliance		Accountable information systems and decisions, Content value, tagging and enrichment **Accountability**	Accountability, Distributed Authority of republished materials	Developing transparency	Trust: Transparency	Trust: Transparency
7. Respect for User Privacy Keep it User Centric **Privacy**	1. Consent 6. Accuracy 9. Access **Consent**		End user-centered systems, personalization, middle-out ontology approach	Consent , Integrity, Content and added value preservation	Accuracy	Aggregated value	Accuracy of the information

Users as Individuals

Data

Providers

Process

Users as People

Users as Reporting People

I CIVIL RIGHTS

II GLOBAL RIGHTS

III LEGAL RIGHTS

IV PROCEDURAL RIGHTS

V DIGITAL RIGHTS

DERECHO RELACIONAL

- La distribución de expectativas sobre la inteligencia social en términos de derechos y deberes en un marco tecnológico
- La interacciones entre los usuarios, y las interacciones entre ellos, los programas y las interfaces humano-máquina crean un valor añadido que facilita la emergencia de la conexión entre la Web 2.0 y la Web 3.0.
- Confianza, seguridad, diálogo, transparencia… y no sólo la identidad cuentan para ello, y deben asumirse como rasgos de los modelos regulativos.
- Esto constituye el nicho ecológico en el cual distintos tipos de tecnología y agentes (ya sean humanos o artificiales) convergen para lograr un resultado común.

CONCLUSIONES

- Redefinición de lo real y lo virtual: híbridos (tecnología cognitiva)
- Los modelos reguladores no sustituyen al derecho: lo rearticulan, reformulan y modelan en función de los usuarios, la arquitectura y las interfaces
- La arquitectura y las interfaces constituyen los dos polos de una estructura regulativa con la que ya estamos viviendo
- La inteligencia social (y no solo el comportamiento individual) constituye nuevos campos regulativosque definen un nuevo objeto jurídico
- Necesitamos nuevos conceptos: *derecho relacional, derecho agregado, derecho desreferenciado* etc…
- Los dos polos de la seguridad y la libertad siguen constituyendo nuestro ámbito de reflexión

Gracias por su atención!

http://31.media.tumblr.com/69eb4f42d0a0973c0fa3ae601355f9e4/tumblr_micgqjbzwt1qg39ewo1_500.gif