Cuando en la sentencia SQL necesitemos introducir valores parametrizados, podemos utilizar el método **prepare** indicando en la consulta con el signo ? para establecer donde serán ubicados, especificando luego una lista de los mismos. El driver PDO se encargará de realizar un escapado correcto de las cadenas, de forma que se evite la posibilidad de una inyección de código SQL malintencionado.

```
$stmt = $db->prepare("SELECT * FROM table WHERE id=? AND name=?");
$stmt->bindValue(1, $id, PDO::PARAM_INT);
$stmt->bindValue(2, $name, PDO::PARAM_STR);
$stmt->execute();
$rows = $stmt->fetchAll(PDO::FETCH_ASSOC);
```

También es posible utilizar marcadores con nombre mediante el caracter **:**, de manera que luego enlacemos cada nombre con el valor por el que será sustituido.

```
$stmt = $db->prepare("SELECT * FROM table WHERE id=:id AND name=:name");
$stmt->bindValue(':id', $id, PDO::PARAM_INT);
$stmt->bindValue(':name', $name, PDO::PARAM_STR);
$stmt->execute();
$rows = $stmt->fetchAll(PDO::FETCH_ASSOC);
```

Es posible en ambos casos enlazar los datos en la propia sentencia **execute**.

```
$stmt = $db->prepare("SELECT * FROM table WHERE id=:id AND name=:name");
$stmt->execute(array(':name' => $name, ':id' => $id));

$rows = $stmt->fetchAll(PDO::FETCH_ASSOC);
```